PARTS OF THE ORIGINAL DOCUMENT

ARE OF POOR REPRODUCTIVE QUALITY

CERTAINES PARTIES DU DOCUMENT ORIGINAL

SONT DE PIÈTRE QUALITÉ DE REPRODUCTION

Programs
Branch
User
Report

RESEARCH ON WHITE COLLAR CRIME: EXPLORING THE ISSUES

NO. 1985-07

Ministry of the Solicitor General of Canada

Secretariat

87-05328/

S.E. Varette
C. Meredith
R.B. Robinson
D. Hoffman
Abt Associates of Canada

RESEARCH ON WHITE COLLAR CRIME: EXPLORING THE ISSUES

NO. 1985-07

This working paper was prepared under contract for the Research Division and is made available as submitted to the Ministry. The views expressed are those of the authors and are not necessarily those of the Ministry of the Solicitor General of Canada. This working paper may not be published, cited or reproduced without permission of the Ministry.

This working paper is available in French. Ce document de travail est disponible en français.

TABLE OF CONTENTS

Chapter Page

I INTRODUCTION 1

II EXECUTIVE SUMMARY 2

III REVIEW OF THE LITERATURE 4

A. Introductory comments 4
B. Definitions of white collar crime: an overview 4
C. Taxonomies of white collar crime 9
D. Computer-related offences 18
E. Estimates of the incidence and cost of white collar crimes 21
F. Concluding comments 24

IV SELECTED FEDERAL GOVERNMENT LEGISLATION: OFFENCES AND CONCERNS 26

A. Our approach 26
B. Offences under federal legislation 29
C. Summary 42

V SELECTED PRIVATE SECTOR ORGANIZATIONS: OFFENCES AND CONCERNS 43

A. Introduction 43
B. Relative incidence 44
C. Discussion 52

VI RELATED INDUSTRY PERSPECTIVES 56

A. Introduction 56
B. Accounting 56
C. Computer security 59
D. Industrial security 62
E. Insurance 63
F. Legal issues 64
G. Other related organizations 69

Chapter **Page**

VII OPTIONS FOR FURTHER RESEARCH 73

A. Introduction 73
B. Policy considerations 73
C. The American experience 76
D. Potential research strategies 80

APPENDICES

A. Lexicon
B. Statistical data
C. Corporate interview guide
D. Notes
E. Bibliography

I

INTRODUCTION

The potential impact of white collar crime, both economically and socially, has triggered increasing concern among criminal justice officials. However, many obstacles prevent a clear approach to the problem. To list just a few:

- The concept itself is vaguely and variably defined.
- Criminal justice statistics reflect only a partial and disaggregated measure of incidence.
- Immediate effects can be diffuse and frequently unknown to the victim.
- The incentive to report and prosecute offences is low in many cases.

This study addresses the feasibility of conducting research that recognizes these obstacles, yet provides usable information for investigation and enforcement activities. For example, identifying relative incidence and loss, if feasible, could improve the allocation of resources to such activities.

The following chapters describe the stages of our research from initial conceptualization to recommendations for future research. Specifically:

- Chapter II highlights the study's key findings and recommendations.
- Chapter III summarizes our directed review of the literature.
- Chapter IV reviews our survey of offences against selected federal legislation.
- Chapter V discusses our findings in the private sector.
- Chapter VI reports on related industry perspectives.
- Chapter VII outlines strategies for future research in the context of perceived policy questions.
- Interview guides, statistical data, a lexicon of unfamiliar terms, and bibliography are appended.

II

EXECUTIVE SUMMARY

Criminal justice officials need better information about white collar crime. But many obstacles prevent a clear approach to the problem. This report examines what kinds of information would prove useful for investigation and enforcement activities.

Our study began with a directed review of the literature. Of particular interest were attempts to operationally define white collar crime and discussions of empirical research. A number of definitions recur throughout the literature, most containing common elements. The specific definition used dictates the nature of offences and the offender. Indeed, even the same definition can generate different taxonomies depending on the user's orientation or concerns (e.g., victims, offenders, the legal system, etc.).

We feel that the following definition adapted from Edelhertz (1970) provides a good starting point for research:[1]

> White collar offences are criminal or quasi-criminal acts or omissions committed without physical force or its threat, that lead to obtaining money, property, information, or other forms of business or personal advantage.

By eliminating specific reference to such qualifiers as concealment and guile, established criminal status of the act and the occupational or corporate role of the offender, we hope to encourage a more exploratory approach while still providing some structure.

Computer crime, for our purposes, is best seen as a dimension of white collar crime in which the computer can play a variety of roles — as the object of the attack, as a necessary tool or as a useful but not essential means.

Reliable information is clearly lacking on the context and incidence of clearly-defined types of white collar crime in Canada. In the United States, most efforts to attach dollar figures to the extent of white collar wrongdoing have focused on the economy as a whole. However, the reliability of these estimates is questionable. Our review of this essentially American literature warns us against taking such a broad-gauged approach: such aggregated figures provide little more than shock value.

A number of Canadian federal government departments have mandates to investigate compliance with federal legislation. Our research included a survey of activity and concerns in areas such as consumer fraud, income tax fraud, unemployment insurance fraud and several others. Some of these offences are treated as crimes; others are not. The potential loss to society as a result of these offences could be considerable. But the dividing line between intentional and unintentional non-compliance is often not apparent. In most cases, government departments recognize that their available resources generate a certain level of effort with outcomes that are predictable. They are generally aware of the behaviour they wish to prevent and direct their efforts — through investigation, prosecution and legislative amendments — towards that end.

We also attempted to gain a general understanding of the private sector's views on white collar crime: its incidence, costs and the ability of existing internal and legal structures to deal with offenders. To this end, we interviewed representatives of approximately 20 organizations from nine roughly-defined industry sectors. Respondents indicated the severity of 10 pre-selected offence types relative to their firm or industry. Our small sample sizes prevent generalization from the results, but do provide some interesting qualitative insights. The most frequently reported concerns were employee pilferage or theft; employee petty larceny and expense account frauds; commercial bribery and kickbacks; and embezzlement or self-dealing. Several types of activities not included in our taxonomy are also problematic. Many of these stem from developments in technology — e.g., unauthorized reproduction of audio or visual materials, illegally "interconnected" equipment in the telecommunications industry, theft of computer time.

Our private sector respondents overwhelmingly prefer to deal with detected offenders internally rather than through the formal legal system. Many firms report increased emphasis on internal security measures. The firms surveyed perceive needs for legislative changes related to computers, copyright and securities.

To complete our overview of white collar crime issues in Canada, we approached representatives of occupations and businesses concerned with the prevention and detection of white collar crime, as well as with mitigating its effects when it does occur. Specifically, we identified the role and interests of accountants, computer security consultants, industrial security managers, insurance firms, the legal community and related institutional bodies. Based on this review, it appears that the work of forensic auditors and computer security analysts might have an important contribution to make.

Finally, we reviewed past research initiatives in the United States and set out a number of options for future research.

III

REVIEW OF THE LITERATURE

A. INTRODUCTORY COMMENTS

The subject of white collar crime has received considerable attention since the concept was first introduced by Sutherland in 1949.[2] A large body of literature exists, most of it produced over the last 15 years. Consequently, we needed to focus our search to satisfy the needs of the feasibility study. Two criteria guided our review of this literature:

- Attempts to operationally define white collar crime.
- Discussions of empirical research on white collar crime, particularly those dealing with measurement of incidence.

B. DEFINITIONS OF WHITE COLLAR CRIME: AN OVERVIEW

Most discussions of white collar crime begin by addressing the thorny issue of definition. Frequently authors will select components from a number of existing definitions, shaping the final product into an instrument that suits their orientation and research needs.

Exhibit III-1 presents a sampling of definitions from the literature. Each contains elements which dictate the nature of offences and offenders included. Saxon (1980) notes a number of characteristics which are common to most:[3]

- Offences committed in the course of one's lawful occupation or as part of one's participation in a government program.
- A violation of trust.
- A lack of physical force to accomplish the crime.
- Money, property, or power and prestige as the primary goals of the crime.
- Definite intent to commit the illegal act.
- An attempt to conceal the crime, usually by passing it off as a normal, legal business transaction or by using one's power and resources to prevent its detection or prosecution.

The particular mix of characteristics in any one definition dictates how broad or restricted the focus of research becomes.

Exhibit III-1. White collar crime: alternative definitions

Author(s)	Definition	Definitional elements/restrictions
1. Clinard and Quinney (1973)	Includes both occupational crime and corporate crime. Occupational crimes are "offences committed by individuals for themselves in the course of their occupations and the offences of employees against their employers." Corporate crimes are "offences committed by corporate officials for their corporation and offences of the corporation itself." The victims for both sub-types are the general public or consumers.[4]	Tends to focus on legitimate occupational and corporate activities, excluding situations where the trust violated has been established in a scam. Also, oriented towards violation of the criminal law thereby overlooking a wide of non-criminal offences. The victim category excludes other corporations and government programs as potential targets.
2. Edelhertz et al (1970)	"An illegal act or series of illegal acts: - committed by non-physical means and by concealment or guile - to obtain money or property - or to obtain business or personal advantage."[5]	Raises the question of what consitutes illegality -- i.e., criminal, quasi-criminal, civil? Is intent required? The criterion of "concealment and guile" could be interpreted to limit white collar to a sub-specie of fraud, there-by eliminating other potentially important offences. Excludes theft of information.

Exhibit III-1. White collar crime: alternative definitions (continued)

	Author(s)	Definition	Definitional elements/restrictions
3.	Reiss and Biderman (1980)	"Those violations of law:	Excludes types of computer crimes where specific penalities have not yet been attached.
		- to which penalities are attached	
		- that involves the use of a violator's position of significant power, influence or trust in the legitimate economic or political institutional order	Criterion of significant power, influence or trust in a legitimate institution may rule out a number of important offenders (eg., embezzlement by bank tellers, securities frauds).
		- for the purpose of illegal gain	
		- or to commit an illegal act for personal or organizational gain."[6]	
4.	Sparks (1979)	"Crime as business" - those crimes which:	Argues for a industry or sector-based analysis; takes a position which is too restrictive for exploratory research.
		- "are carried out primarily for economic gain and involve some sort of commerce, industry, trade or legitimate profession . . .	Determination of segments of the economy for analysis becomes problematic without preliminary evidence.
		- necessarily involve some sort of formal organization or more or less formal relationships between the parties involved . . .	The criteria of formal relationships and legitimate business techniques seem to eliminate some offences of interest (eg., computer crime perpetrated from outside the organization).
		- necessarily involve either the use, or misuse, of legitimate forms and techniques of business, trade or industry."[7]	

Exhibit III-1. **White collar crime: alternative definitions** (continued)

Author(s)	Definition	Definitional elements/restrictions
5. Sutherland (1949)	"A crime committed by a person of respectability and high social status in the course of his occupation."[8]	Introduces difficulties of operationalizing "respectability" and "high social status." Limits offences to those which are legally crimes, those carried out by persons (i.e., not organizations) and by persons in their occupations (i.e., excludes some offences against government).
6. U.S. Department of Justice	"Those classes of non-violent, illegal activities which principally involve traditional notions of deceit, deception, concealment, manipulation, breach of trust, subterfuge or illegal circumvention."[9]	Excludes cases where no attempt at concealment is made. Otherwise so broad that it would not be useful as a guide to the particular contexts of white collar crime.

Sutherland's original definition of white collar crime limited it to lawbreaking committed by respectable people with high social status in the course of their occupation. More recent definitions have expanded the set of actors and acts. But they still generally exclude major classes of crime variously known as street crime, organized crime and common crime, including crimes of "passion." The major variations in the concept since Sutherland's time appear to be that:

- The evolution of technology and mass communications has given all strata of society access to the requisite machinery once only available to the wealthier classes (Bequai, 1978).[10]
- The act does not have to occur within the context of the offender's occupation (e.g., income tax fraud).
- The white collar criminal might well be a corporate entity failing to adhere to one of the growing number of regulations.

These points highlight three recurring themes in definitions of white collar crime which Shapiro (1980) examines in relation to their empirical value: the social status of offenders, the social location of offences and the criminality of the offences.[11]

The very term "white collar" reflects the concept of social status by alluding to individuals in positions of respect and responsibility. Shapiro argues that little insight is gained by isolating the status of white collar offenders: the correlation of status with other factors (e.g., the nature of opportunities to commit misdeeds afforded by the individual's position) contributes more to an understanding of categories of wrongdoing. Consequently, these other factors emerge as important variables.

Shapiro also questions the utility of focussing on the social location of offences. Some definitions identify white collar crime as crime that takes place in one's occupational setting. Such a criterion introduces ambiguities in identifying what constitutes an appropriate setting and appropriate activities for investigation within that setting. At the same time, it may restrict the scope of the definition unnecessarily.

These concerns suggest that components of traditional definitions contribute little to an empirical approach. Moreover, in their orientation towards individual behaviour, they underemphasize a major dimension of white collar crime — new opportunities for illegality generated by organizations. According to Shapiro:

> Organizations create opportunities for illegality:
>
> 1) By serving as wealthy and relatively accessible victims.

> 2) By expanding the scope of transactional systems and generating impersonal transactions and their related forms of abuse.
>
> 3) By creating and allocating resources and opportunities, the exploitation of which is desirable to organizational insiders and outsiders.
>
> 4) By providing a strategic device to facilitate and cover-up illegalities.
>
> 5) By conditioning the development of new normative prescriptions capable of breach.
>
> Offences may reflect the victimization of the organization by the individual, the exploitation of organizational opportunities for individual enrichment, the collaboration of organization and individual in illegality, or the breach of norms pertaining to organizational behaviour by organizations and persons in organizational roles. In any case, organizations multiply the opportunities for violation, the strategies of offence, and the chances of cover-up. It is this new stage for the drama of violative activity that is implicit in social location, and it is the drama itself that is the substance of white collar crime. (p.10)

In other words, a definition of white collar crime might more usefully focus on collective opportunities rather than linking a particular offence to an individual's status or occupation.

Finally, Shapiro argues that the definitional debate over the criminal designation of white collar offences is "trivial and arbitrary" (p. 27). Adhering too closely to current legal norms removes from the researcher's perspective many of the most important questions about white collar wrongdoing.

How do these observations contribute to our study? Primarily by recommending a flexible, dynamic approach. Since we hope to develop measures to identify the scope and relative incidence of white collar crime, an overly restrictive definition is counter-productive. At the same time, the absence of structure will reduce the practical value of any definition.

C. TAXONOMIES OF WHITE COLLAR CRIME

Definitions are valuable when they bound a problem and provide a reference point. But the specific use of a definition depends largely on the user's needs or interests. To illustrate, the Edelhertz definition forms the basis of at least three overlapping, but nonetheless different, taxonomies.

1. Edelhertz's categories of white collar crime

Edelhertz develops categories of criminal activity that tend to emphasize the offender and context:

- Crimes by persons operating on an individual, ad hoc basis.
- Crimes in the course of their occupations by those operating inside business, government, or other establishments, in violation of their duty of loyalty and fidelity to employer or client.
- Crimes incidental to and in furtherance of business operations, but not the central purpose of the business.
- White collar crime as a business, or as the central activity.

These four categories generate the list of activities shown in Exhibit III-2. (Unfamiliar terms in the Exhibit and throughout the balance of the report are explained in the lexicon -- Appendix A.)[12]

2. The U.S. Attorney General's taxonomy

Endorsing a definition combining those of Edelhertz and the U.S. Department of Justice, the Attorney General sets out a number of victim-oriented categories of white collar criminal activity:

- Threatening the integrity of government institutions and processes.
- Defrauding the government, reducing the effectiveness of government programs and resulting in higher government and taxpayer costs.
- Victimizing business enterprises.
- Victimizing consumers.
- Victimizing investors and the integrity of the marketplace.
- Victimizing employers.
- Threatening the health and safety of the general public.[13]

Again, a number of specific types of offences fall under each of these headings.

Exhibit III-2. Edelhertz: categories of white collar crimes

A. Crimes by persons operating on an individual, ad hoc basis

1. Purchases on credit with no intention to pay, or purchases by mail in the name of another.
2. Individual income tax violations.
3. Credit card frauds.
4. Bankruptcy frauds.
5. Home improvement loan frauds.
6. Frauds with respect to social security, unemployment insurance, or welfare.
7. Unorganized or occasional frauds on insurance companies (theft, casualty, health, etc.).
8. Violations of Federal Reserve regulations by pledging stock for further purchases, flouting margin requirements.
9. Unorganized "lonely hearts" appeal by mail.

B. Crimes in the course of their occupations by those operating inside business, Government, or other establishments, in violation of their duty of loyalty and fidelity to employer or client

1. Commercial bribery and kickbacks involving buyers, insurance adjusters, contracting officers, quality inspectors, government inspectors and auditors, etc.
2. Bank violations by bank officers, employees, and directors.
3. Embezzlement or self-dealing by business or union officers and employees.
4. Securities fraud by insiders trading to their advantage by the use of special knowledge, or causing their firms to take positions in the market to benefit themselves.
5. Employee petty larceny and expense account frauds.
6. Frauds by computer, causing unauthorized payouts.
7. "Sweetheart contracts" entered into by union officers.

Exhibit III-2. Edelhertz: categories of white collar crimes (continued)

8. Embezzlement or self-dealing by attorneys, trustees and other persons in positions of confidence or trust.
9. Fraud against the government.
   a) Padding of payrolls.
   b) Conflicts of interest.
   c) False travel, expense or per diem claims.

C. Crimes incidental to and in furtherance of business operations, but not the central purpose of the business

1. Tax violations.
2. Antitrust violations.
3. Commercial bribery.
4. Food and drug violations.
5. False weights and measures by retailers.
6. Misrepresentation of credit terms and prices.
7. Submission or publication of false financial statements to obtain credit.
8. Use of fictitious or over-valued collateral.
9. "Cheque-kiting" to obtain operating capital on short term financing.
10. Securities Act violations, i.e., sale of non-registered securities, to obtain operating capital, false proxy statements, manipulation of market to support corporate credit or access to capital markets, etc.
11. Collusion between physicians and pharmacists in the writing of unnecessary prescriptions.
12. Dispensing by pharmacists in violation of law, excluding narcotics traffic.
13. Immigration fraud in support of employment agency operations to provide domestics.

Exhibit III-2. Edelhertz: categories of white collar crimes (continued)

14. Housing code violations by landlords.
15. Deceptive advertising.
16. Fraud against the government:
    a) False claims.
    b) False statements (eg., to obtain loans).
17. Labor violations.
18. Commercial espionage.

D. **White-collar crime as a business, or as the central activity**

1. Medical or health frauds.
2. Advance fee swindles.
3. Phony contests.
4. Bankruptcy fraud, including schemes devised as salvage operation after insolvency of otherwise legitimate businesses.
5. Securities fraud and commodities fraud.
6. Chain referral schemes.
7. Home improvement schemes.
8. Debt consolidation schemes.
9. Merchandise swindles (eg., pyramid clubs).
10. Land frauds.
11. Directory advertising schemes.
12. Charity and religious frauds.
13. Personal improvement schemes (eg., fraudulent diplomas).
14. Fraudulent application for, use and/or sale of credit cards, airline tickets, etc.
15. Insurance frauds.

Exhibit III-2. Edelhertz: categories of white collar crimes (continued)

16. Vanity schemes.

17. Ponzi schemes.

18. False security frauds.

19. Purchase of banks, or control thereof, with deliberate intention to exploit their assets illegally.

20. Fraudulent establishing and operation of banks or savings and loan associations.

21. Fraud against the government:

    a) Organized income tax refund swindles, sometimes operated by income tax "counsellors."

    b) Exporting of totally worthless goods insured by government.

    c) Frauds against federal housing legislation:

        - Obtaining guarantees of mortgages on multiple family housing far in excess of value of property with foreseeable inevitable foreclosure.

        - Home improvement frauds.

22. Executive placement and employment agency frauds.

23. Coupon redemption frauds.

Source: Edelhertz (1970, pp. 73-75).

3. The Shapiro typology

Shapiro suggests that the Edelhertz definition leads one to categorize most offences as one (or more) of:

- Fraud -- perhaps the clearest category, involving the use of deception, the misrepresentation of status, experiences, commodities, or future events for the purpose of diverting economic assets from the receivers of misrepresented information to its sources.
- Self-dealing -- reflects the opportunities afforded in organizational positions to expropriate resources. The central distinguishing feature is the location of offenders in positions of trust and the exploitation of these positions for personal enrichment. The typical examples of offences in this category are embezzlement, pilferage, and employee theft. They pertain to the expropriation of commodities that are specifiable and fixed in quantity, whose gain constitutes a loss to other parties.
- Corruption -- similar in context to self-dealing, but where insiders direct assets and opportunities to outsiders because of incentives they are offered.
- Regulatory offences -- the violation of administrative regulations pertaining to the conduct of business, the use of public facilities, or the obligations of citizenship. Examples of such rules include the payment of taxes; licensing and registration of organizations, professionals, equipment, securities issuances, and the responsibilities of registrants; the conditions of employment (concerning hours, wages, safety, and discrimination); the relationship between organizations and their environment and the relationship between organizations themselves with regard to antitrust, bid-rigging, referral schemes, etc.[14]

Shapiro, in contrast to the other two sources, skirts the criminality issue by interpreting illegality quite broadly. To draw a further distinction, her taxonomy highlights the nature of the offence as opposed to offender, location or victim.

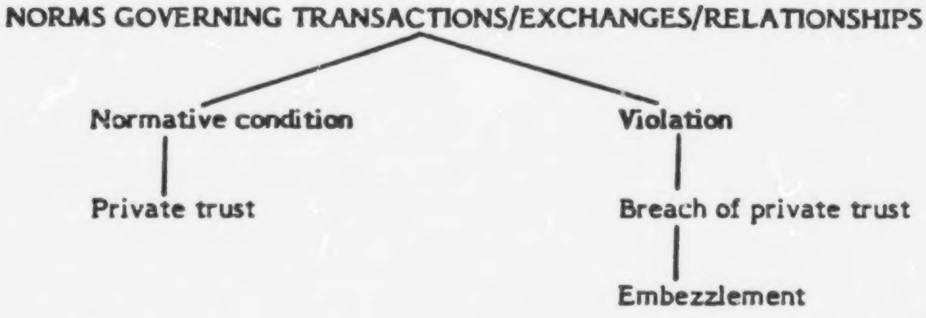
Reiss and Biderman (1980) propose two novel systems for classifying white collar crime.[15] The first is based on types of normative systems (e.g., free competitive market norms) which in turn proscribe related properties and violations (e.g., illegal monopoly, price conspiracy). Their second classification system is based on three major dimensions of normative control:

- Norms governing transactions, exchanges or social relationships.

- Norms governing the status of organizational or collective states.

- Norms covering the social control of violations.

Each normative dimension has a set of normative conditions which can be violated, which in turn have characteristic violations. This flow is illustrated below:



Since this approach addresses all kinds of offences, its specific value to classifying white collar crime is somewhat limited.

Yet another perspective to ordering white collar wrongdoing is by degree of legality. In a background paper prepared for the Sixth United Nations Congress on Prevention of Crime and Treatment of Offenders, Avison (1980) constructs a matrix of activities and actors. Within this matrix, one can identify opportunities for "gilded" criminals to abuse economic and social power (see Exhibit III-3). Each cell contains activities defined by actor and legitimacy. Avison lists most offences typically included in taxonomies of white collar crime under Column C, cells nine and ten. Yet, a study concerned with legal issues (i.e., existing legislative constraints) might include activities under Columns B and D.

The variety of existing taxonomies of white collar crime has several implications:

- Despite commonly held definitional parameters, decisions on activities to be included reflect particular orientations or concerns (e.g., victims, offenders, the legal system, etc.).

- Activities listed can range from broad behavioural descriptions to specific criminal infractions.

EXHIBIT III-3. Framework for categorizing activities by degree of legality

Agency Acting	Type of Activity (or Omissions)			
	Legitimate & socially not problematic (A)	Legitimate but socially problematic (B)	Not legitimate, illegal & socially problematic (C)	Illegal but perhaps socially desirable (D)
Individual person	1	5	9	13
Organization established to pursue socially approved goals	2	6	10	14
Organization established to pursue illegal or non-legitimate goals	3	7	11	15
Governments and agencies of government	4	8	12	16

Source: Avison (1980, p.5).

- The choice of a closed over an open-ended approach involves assumptions about the nature of white collar crime and predetermines the focus of the research.

D. COMPUTER-RELATED OFFENCES

Computer-related offences can be conceptualized in two ways, not mutually exclusive:

- As a subset of computer abuse.
- As a new form of white collar crime.

1. Computer crime as a subset of computer abuse

Parker (1980) identifies the following kinds of computer abuse:

- Vandalism.
- Information or property theft.
- Financial fraud or theft.
- Unauthorized use or sale of services.

He distinguishes between types of abuse depending on the use made of the computer itself:

- "Inspec" - where the abuse involves authorized kinds of activity directed to an unauthorized end. Manipulation of data input or output is often involved e.g., a bank teller embezzling by transferring funds among accounts by means of an on-line terminal. Perpetrators tend to be those whose skills and knowledge are not primarily in the computer area.
- "Nonspec" - where the abuse involves the use of computers in unauthorized ways, or not according to the specifications or instructions for their use. This would include:
    - .. Unauthorized changes to software.
    - .. Use of software to modify the content of the data files in computers in unauthorized ways.

  Perpetrators are likely to have skills and knowledge in computer technology.

Nycum (n.d., pp. 271-272) has proposed the following taxonomy for analyzing software abuse:

- Misappropriation of software by utilization of a remote terminal:
  - For example, a recent (U.S.) case involved fraudulent access to a computer, copying of protected software and removal of the copy - all from a remote terminal.
- Misappropriation of software by direct access to a computer centre or software storage facility:
  - Unauthorized or fraudulent access to software by an unprivileged user who has no authorized access to software.
  - Unauthorized fraudulent disclosure of proprietary software by an employee or former employee or contract program developer.
- Obliteration or bugging of software:
  - Includes physical damage to disc drives causing obliteration of information, magnetic obliteration of information on magnetic tapes or interference with the designed use of the software by trick or artifice not causing actual obliteration.
- Miscellaneous other abuses:
  - Other antisocial behaviour directly or indirectly involving software may give rise to prosecutions (in the U.S.) for fraud and embezzlement, credit card abuse, forgery, robbery or receiving stolen property.

In other words, this approach defines computer crime as that subgroup of computer abuses that are criminal in nature. However, the dividing line is not entirely clear. The criminal code as it currently stands does not deal adequately with some types of computer-related wrongdoing. As a tool for guiding research, then, this conceptualization is of limited value.

2. Computer crime as a new form of white collar crime

Computer crime can also be viewed as essentially a new dimension in white collar crime in which:

- The perpetrators use new skills, knowledge, and means of access to assets.

- The environments include not only computer centres and remote terminals but also the inside of computers and the communication circuits used.

- The modi operandi include a whole variety of techniques unique to the computer, some of which are currently impractical to detect or prevent. For example, the "salami" method involves automatically deducting small amounts from several bank accounts and depositing the funds in an account set up by the offender.

- The forms of assets include the usual assets plus many new forms: secret information, records representing physical assets, computers and computer services, and software.

- Timing -- the criminal act usually takes place in two time dimensions: real time, when the perpetrator performs the necessary physical acts and nonreal (i.e., computer) time, when the computer responds. Moreover, the computer's response, measurable in fractions of seconds, may be automatically repeated periodically over weeks, months, and years.

- The perpetrator need not be in geographic proximity to the locus of the criminal act (Parker, 1980).

In fostering this new dimension of white collar crime, the computer can play a variety of roles in the act itself:

- As the object of the attack when vandalism or sabotage of hardware or software occurs.

- As the primary instrument of the act.

- As a symbolic entity to which people can either attach blame or innocence. For instance, a computer might intimidate, deceive or defraud victims - such as when a company fraudulently re-invoices another for a debt already paid and when discovered, claims that it was a "computer error." Conversely, computer-generated data may be credited with an unwarranted degree of authenticity -- i.e., there is a tendency not to question computer printouts.

This approach defines computer crime as a subset of white collar crime by differentiating the roles the computer can play. In doing so, it leads to the important research question of whether the concept is a meaningful one in terms of ordering white collar crime.

E. ESTIMATES OF THE INCIDENCE AND COST OF WHITE COLLAR CRIME

Most efforts to attach dollar figures to the extent of white collar crime have focussed on the American economy. Saxon (1980) highlights a number of these attempts:

- In 1974, the U.S. Chamber of Commerce estimated the short-term direct cost of white collar crime to the U.S. economy to be no less than $40 billion annually (see Exhibit III-4).
- In 1976, the Joint Economic Committee of the U.S. Congress estimated the cost of white collar crime to be $44 billion annually.
- In 1977, the American Management Association estimated that non-violent crimes against business firms cost $30-$40 billion per year (see Exhibit III-5).
- In 1978, the U.S. General Accounting Office estimated the loss from fraud in government programs to be between $2.5 and $25 billion per year.[16]

However, the reliability of these estimates is questionable. The U.S. Chamber of Commerce figure excludes anti-trust violations and the consequences of white collar crime which violates health and safety standards. In addition, this figure includes costs associated with shoplifting, not a white collar crime by any definition unless committed by employees.

The figure of $44 billion cited by the Economic Committee of Congress was obtained by correcting the Chamber of Commerce estimate for inflation.

The American Management Association's approximate total of $30-40 billion does not consider the costs of bribery and overseas payoffs by corporations.

Estimates of the cost of computer crime have also been made. Parker (1976) estimated that the annual losses worldwide due to computer-related misdeeds would be approximately $300 million.[17] Taber (1980) has sharply criticized Parker's figure:

> The SRI (Parker) study is unreliable because it is based on poor documentation, unacceptable methods, and unverified (indeed unverifiable) losses. In addition, it is unfocussed, and inconsistent within its own definitions and terminology, which are themselves disputable. (Based on these methods)... Parker got an average loss of $450,000 per 'computer crime' case. SRI derived the estimated annual loss of $300 million based on this average and the following unwarranted assumptions:

EXHIBIT III-4. Breakdowns of estimates of white collar crime (in billions)

The U.S. Chamber of Commerce		The American Management Association	
Bankruptcy fraud	$ .08		
Bribery, kickbacks and payoffs	3.00	Commercial bribery and kickbacks	$3.5-10
Computer-related crime	.10	Burglary	2.5
Consumer fraud, illegal competition, deceptive practices (excluding price-fixing and industrial espionage)	21.00	Vandalism	2.5
Credit card and cheque fraud	1.10	Credit card fraud	.50 million
Embezzlement and pilferage	7.00	Employee pilferage	5.00-10.00
		Embezzlement	4.00
Insurance fraud	2.00	Shoplifting and insurance fraud	4.00
Receiving stolen property	3.50		
Securities thefts and frauds	4.00	Securities thefts and fraud	5.00
TOTAL	$41.78[1]	TOTAL	$27-38[1]

Source: Saxon (1980), pp.8-10.

[1] Some categories not mutually exclusive (eg., part of the computer-related crime estimate may also be included in the embezzlement figure).

> - Assume an average of 100 cases per year (reported). Assume also that only 15% of known cases are reported. With an average loss of $450,000, a total annual loss...would be $300 million.
>
> There is no good reason to accept any of these assumptions; one hundred cases a year is the asymptote of SRI's projection of reported cases in the media based on the past experience of SRI in its gathering of these articles. There is no reason given for the 15% figure. And $450,000 is highly questionable. In sum, neither $450,000 nor $300 million have a shred of validity. (p.309)

According to Watkins (1981), the assumption that 85% of computer crime is undetected derives from a 1976 study which showed that 85% of violent crimes in Detroit are unreported. He also points out that not only is the leap of logic to computer abuse unsound, it is also not supported by the experience of representatives in industries required by law to report any crime occurrence. Watkins claims that approximately 75 computer abuse cases are reported annually, representing .02% of computer installations. The obvious question of how many go unreported arises. But Watkins responds by noting the few computer crimes recorded by the Canadian Bankers Association which has a requirement that members report fraud and embezzlement cases.[18]

Burns International Security Services Inc. used loss projections for 1981 to estimate that between 1800 and 2700 computer crimes (undefined) will be committed this year at a cost of $1.2 to $1.8 billion ("Computer Crimes Increase," Globe and Mail, August 1981). Given the methodological concerns over how Parker's derived his $300 million figure, the Burns figure is also suspect.

Aside from efforts to produce overall cost estimates, other studies have looked at levels of incidence, usually focussed more narrowly. Sutherland's original work examined corporate crime among some of the largest organizations in the United States: several violations of law were cited for each. After a considerable time gap, Clinard et al. (1979) completed the first comprehensive study of corporate violations since Sutherland's work (Saxon, 1980). The Clinard study reported that over a two-year period, more than 60% of 582 of the largest publicly owned U.S. corporations had at least one legal action initiated and one enforcement action completed against them.

A recent study sponsored by the National Institute of Law Enforcement and Criminal Justice with the assistance of the American Management Association examined employee theft in 35 businesses covering the retail, manufacturing and hospital sectors. Using self-completed questionnaires and interviews, Clark and Hollinger (1981) were able to relate the incidence of employee theft with employee characteristics and the presence of controls.[19]

Surveys of the public have tended to focus on the perceived seriousness of white collar crime. After analyzing one such survey, Schrager and Short (1980) suggest that the delayed and diffuse effects of many white collar crimes reduce the public's awareness of their impacts.[20] This observation perhaps explains the lack of victimization surveys aimed at identifying individual victims of white collar crime.

Their broad underlying assumptions and variability in the rigour of data collection suggest that American figures on cost and incidence should be regarded as rough estimates at best. Research in Canada has not even progressed to this rough stage of measurement. Our review of the literature did not reveal any Canadian studies dealing with these issues in a broadly-based and empirical way.

Formal crime reports add little to our understanding. The Justice Statistics Division of Statistics Canada reports on three broad categories of fraud only:

- All false pretence, forgery, uttering (circulation of counterfeit money) and fraud offences involving cheques.

- All such offences involving credit cards.

- All other such offences.

Many of the specific offences falling under these categories would not generally be classified as white collar crime. Also, the statistics available on these categories are based on police reports and are limited to offences covered by the criminal code. As such, they can provide only a partial picture of the extent of white collar illegality in Canada.

One potential vehicle for addressing these "shortcomings" of the justice statistics reporting system is the recently created Canadian Centre for Justice Statistics. Given the Centre's general concern with producing national statistics to inform criminal justice policy planning it should perhaps be encouraged to:

- Gather and report data on fraud in more detail than the three categories noted above can provide.

- Gather and report data on compliance with federal and provincial regulations (e.g. consumer legislation, welfare abuse).

F. CONCLUDING COMMENTS

Our selected review of the literature leads us to some preliminary research positions. We agree with Shapiro (1980) that we should "move away from questions of definition and closer to concern for differentiation and analysis." But we feel that the following definition adapted from Edelhertz provides a good starting point for research:

> White collar offences are criminal or quasi-criminal acts or omissions committed without physical force or its threat, that lead to obtaining money, property, information, or other forms of business or personal advantage.

By eliminating specific reference to such qualifiers as concealment and guile, established criminal status of the act and the occupational or corporate role of the offender, we hope to encourage a more exploratory approach while still providing some structure.

Our review of the essentially American literature dealing with costs and incidence of white collar crime warns us against taking such a broad-gauged, ill-defined approach. Large figures covering a whole economy provide little more than shock value. To be useful, such research should apply a general definition such as the one just proposed to manageable units of analysis.

IV

SELECTED FEDERAL GOVERNMENT LEGISLATION: OFFENCES AND CONCERNS

A. OUR APPROACH

Several federal government departments, as well as the R.C.M.P., have mandates to investigate compliance with federal legislation. Many of the Acts that they enforce prohibit activities covered by our proposed definition of white collar crime. Our research included a survey of relevant activity and concerns in a number of departments.

Exhibit IV-1 shows the offences and relevant legislation surveyed. The selection process was entirely subjective. We included offences/legislation suggested by the Steering Committee and added other Acts which also related to the study. However, we emphasize that our search for relevant legislation was by no means exhaustive. The intention was to gather summary data in as many areas as possible to guide our development of future research strategies.

In our contacts with representative officials, we attempted to become familiar with specific offences, clarify mandates and investigative activities, identify any parallel research efforts and gauge potential interest in future research. Most interviews were conducted in person, with a small number completed by telephone. The interviews were largely unstructured, but generally covered the following areas:

- Descriptions of possible offences.
- Mandate of the branch or division responsible for the relevant Act.
- Target groups — potential offenders and victims.
- Means of identifying and investigating offences.
- Distinction between offences treated as crimes and those dealt with as administrative infractions, as well as relative rates of prosecution.
- Estimate of the costs or dollar value of these offences.
- Concerns about the extent of offences not detected.
- Interest in a study which would develop a strategy to measure incidence and losses.
- Comments on the strength of legislation in the area concerned.

EXHIBIT IV-1. Selected offences, related legislation and departments contacted

	Offences	Legislation	Department	Area Contacted
1.	Consumer fraud	Food and Drug Act	Consumer and Corporate Affairs	Bureau of Consumer Affairs
		Packaging and Labelling Act		
		Precious Metals Marketing Act		
		Weights and Measures Act		
2.	Copyright infringement	Copyright Act	Consumer and Corporate Affairs	Copyright & Industrial Design Office
3.	Customs offences	Customs Act	Revenue Canada - Customs and Excise	Adjudications Directorate
		Excise Act		
		Excise Tax Act		
4.	Fraud against income security programs	Canada Pension Plan Act	Health and Welfare	Income Security Programs
		Family Allowance Act		
		Old Age Security Act		
5.	Fraudulent bankruptcy	Bankruptcy Act	Consumer and Corporate Affairs	Bankruptcy Branch

	Offences	Legislation	Department	Area Contacted
6.	Income Tax fraud	Income Tax Act Taxation	Revenue Canada - Research Division	Compliance
7.	Misleading advertising and deceptive marketing practices	Combines Investigation Act	Consumer and Corporate Affairs	Marketing Practices Branch
8.	Non-competitive business behaviour	Combines Investigation Act	Consumer and Corporate Affairs	Bureau of Competition Policy
9.	Offences against government assistance to business	Small Business Loans Act	Industry, Trade and Commerce	Small Business Secretariat
10.	Offences against the environment			
	- Air	Clean Air Act	Environment Canada	Air Pollution Control Directorate
	- Environment	Environmental Contaminants Act	Environment Canada	Environmental Impact Control Directorate
	- Water	Canada Water Act Fisheries Act Ocean Dumping Act	Environment Canada	Water Pollution Control Directorate
11.	Tax rebate discounting offences	Tax Rebate Discounting Act	Consumer and Corporate Affairs	Consumer Services Branch
12.	Unemployment Insurance fraud	Unemployment Insurance Act	Canada Employment and Immigration Commission	Control Programs Directorate

Interview responses in relation to selected offences are discussed below. (They are ordered alphabetically, not according to relative importance). Information is not directly comparable in each instance; the relevance, availability and method of compiling data varied among departments. Again, we remind the reader to treat the following summaries as overviews rather than comprehensive case studies.

B. OFFENCES UNDER FEDERAL LEGISLATION

1. Consumer fraud

The Department of Consumer and Corporate Affairs — through the Consumer Products Branch (formerly the Consumer Fraud Protection Branch) — is jointly or solely responsible for administering a number of federal Acts designed to control consumer fraud. Exhibit B-1 (Appendix B) summarizes the prosecutions made under four of the major consumer protection measures:

- The Food and Drug Act.
- The Weights and Measures Act.
- The Packaging and Labelling Act.
- The Precious Metals Marketing Act.

The success rate in prosecutions seven or eight years ago approached 100%. At that time, nearly everyone prosecuted pleaded guilty. Recent years have witnessed a much higher rate of contested cases and a parallel drop in the ratio of convictions to charges. Perhaps because fines are not substantial, small operators tend to plead guilty. But larger companies are contesting prosecutions in the courts.

Field staff monitor a wide range of business activity for offences against the major consumer protection measures. In many cases, persuasion results in compliance and corrections are made without prosecution. Repeated incidents by the same offender suggest a deliberate attempt to defraud.

Cutbacks have reduced the number of monitoring staff to approximately 200. A combination of compliance profiles (drawn from previous experience) and a "risk to public" factor enables the branch to direct its relatively scarce resources to key industries. Reported non-compliance has been greatest in the dairy industry, followed by fresh and frozen meat, women's wear and grain.

2. Copyright infringement

In Canada, action against copyright infringements falls under civil law procedures. The Copyright Act is not policed and the Department of Consumer and Corporate Affairs has no mandate to do so. One section of the Copyright Act does permit action by the Crown, but until 1973 no action was taken. From 1973 to 1977, the department's activity was very nominal and total fines of only $275 were awarded as the result of prosecution. Since 1978, the Canadian Recording Industry Association and the Canadian Motion Pictures Distributors have been lobbying the department for more effective action on their behalf in dealing with the problem of "pirating" of audio/video cassettes.

The R.C.M.P. has investigated a number of cases, but the question remains as to who should initiate prosecution through the Department of Justice. Moreover, the maximum fine for conviction is only $200 per transaction and up to two months in jail. The multi-million dollar losses claimed by industry have led to considerable pressure for stronger criminal sanctions.

The Department of Consumer and Corporate Affairs is currently trying an omnibus approach to the revision of its copyright legislation.

Under the existing framework, the R.C.M.P. would have to divert resources to prosecute. And they are apparently willing to do so. But the penalties do not warrant extensive investigation and the costs of prosecution.

Violation of copyright can involve:

- Bootlegging, which is the unauthorized recording of a live event.
- Piracy, which is the unauthorized duplication and sale of copyrighted material without apparent effort to present it as the original.
- Counterfeiting, the unauthorized duplication of copyrighted material and its sale in a form as much as possible identical to the original.

Counterfeiting gives rise to the most causes of legal action (torts, unauthorized appropriation of personality, copyright, etc.). Unfortunately, it is the most difficult to discover. Piracy is the easiest to detect, but carries with it only the penalties for violation of copyright under the existing legislation.

The range of offenders varies from individuals violating copyright in the illegal transfer of copyrighted material to a blank tape to organized crime, with an international distribution network, mainly engaged in counterfeit activity. The bogus product is mixed with proper goods and sold at regular retail prices.

Stronger U.S. legislation has made Canada something of a haven for this type of activity. Chapter V deals with these issues from the private sector perspective.

3. Customs offences

The Adjudications Directorate of Revenue Canada, Customs and Excise, rules on offences against the Customs Act and the Excise Tax Act. As well, several other Acts contain provisions for specified activities to be dealt with under the Customs Act.

Three agencies carry out seizures and investigations:

- Ports officials and the R.C.M.P. physically seize goods.
- Customs Investigators carry out commercial investigations after the fact, ascertain offences based on records and demand payment for unlawful importation.

The R.C.M.P. allocates 263 person years to customs work across the country, but investigates less than 50% of cases. A 1932 Order-In-Council gave the R.C.M.P. authority in land smuggling cases. In recent years, an effort has been made to extend this mandate to commercial investigations. The R.C.M.P. handles some cases believed to involve criminal intent now, but the majority are undertaken by the Customs Investigation Service of Customs and Excise.

The Customs Investigation Service, with 105 investigators, carries out approximately 500 investigations per year which may result in a demand for payment or prosecution if intent can be proven. The large number of referrals from Ports officials dictates that investigators concentrate on companies thought to be undervaluing hundreds of thousands of dollars worth of goods.

All three groups report to the Adjudications Directorate which upholds or diminishes penalties and decides on whether to prosecute. Types of offences which may be serious enough to prosecute include:

- Quantities of dutiable goods smuggled for resale.
- Dock workers and stevedores pilfering dutiable goods from cargo.
- Repeated customs infractions of a serious nature by the same individual or company.
- Violation of the Settler's or Returning Resident Regulations.
- Quantities of goods smuggled for use by a commercial firm, not necessarily for resale.

- Deliberate attempts by commercial firms to defraud through deliberate undervaluation, false records, books or invoices.

The Customs Act affords strong remedies: offenders are considered guilty until proven innocent. Administrative penalties — which may include duty, fine and forfeiture — are stiffer than those of many other Acts. Their severity and potential deterrent effects are considerable; consequently, prosecutions are recommended only in the more serious cases.

If an Investigation or Ports official recommends prosecution, the Adjudications Directorate reviews the case and refers it to the Department of Justice to lay charges if warranted. Sections in the Customs Act revert to the Criminal Code for penalties. Indictable offences carry a maximum fine of $5,000 with a jail sentence. Individuals acting within a commercial firm are prosecuted when possible.

Exhibit B-2 shows operational statistics for the Adjudications Directorate for the last two years. Exhibit B-3 provides a statement of revenue related to seizures. These figures may differ from other sources within the department which aggregate the value of all goods seized, including the vehicles used for transportation.

During 1980-81, there were 202 recommendations for prosecutions, 178 convictions and 24 dismissals or withdrawals. These figures reflect the overwhelming use of administrative penalties.

Commercial investigations of firms undervaluing goods are important due to potential revenues lost and the impact on competition. Sectoral characteristics have not emerged.

4. Fraud against income security programs

Comments by Health and Welfare Canada officials suggest that fraud is not perceived to be a major problem, although ignorance or misunderstanding may cause loss.

Since income security payments constitute a means of income distribution, the department adopts a relatively lenient approach to compliance investigation. Fraudulent cases would result in prosecution under the criminal code.

5. Fraudulent bankruptcy

No meaningful estimate of the losses to society due to fraudulent bankruptcy could be produced.

Fraudulent bankruptcy can follow one of two patterns:

- The classic form of criminal activity involves the purchase of a good, sound business; the acquisition of goods on credit from old and new suppliers of the firm; then the declaration of bankruptcy and the disposition of the goods without recovery.
- The second type involves individual businessmen who, facing a bad turn of fortune, "skim" some of the assets of their business before declaring bankruptcy.

The Bankruptcy Branch is considering amendments to the existing legislation. Currently, the Superintendent of Bankruptcy is responsible for identifying prima facie cases of fraudulent bankruptcy. The R.C.M.P. then carries out the prosecution. After all the effort involved, the logic of the situation is to prosecute, regardless of the consequences to the victims of the crime. When convictions are obtained and the guilty are jailed, the possibility of compensating victims disappears with the sudden loss of income. The civil route, which would provide a remedy to victims, is not available.

However, a considerable proportion of the investigations do not lead to criminal prosecution because of insufficient evidence. The criminal activity characteristic of the early sixties appears to be less prevalent now. In only 20% of the cases of "business failure" are the companies formally bankrupt. In most cases, they simply close their doors. Nevertheless, 421 new bankruptcies were assigned to the R.C.M.P. for investigation in 1979 — an increase of 20% over 1978.

6. Income tax fraud

Compliance research under the Income Tax Act focusses on measuring the tax gap, particularly the recoverable gap — that proportion of the absolute gap that could be recovered with existing investigative techniques.

Recoverable non-compliance tax for the 1978 tax year is estimated to be $2.7 billion in current dollars, not including interest. This figure represents the amount recoverable from normal (not in-depth) audits and under-reporting picked up by the computer.

Audits examine only the non-salaried proportion of the population filing returns (i.e., corporations, farmers and fishermen, professionals, others self-employed). This target group numbers approximately five million of the 16 million who file, including all Revenue-Canada Taxation staff who are audited every year. Estimates of the number of non-filers are difficult to make. "Guesstimates" of the total recoverable gap (i.e., if resources were available and tools could be developed) and the absolute tax gap (i.e., including losses that could never be recovered) are $4.5 and $10 billion respectively.

But there are many non-filers who do not warrant investigation. Consequently, the department concentrates on maximizing the efficiency of tax administration by developing work-selection techniques.

Errors or non-compliance are detected at three stages:

- Initial assessment procedures note and correct relatively small errors.
- Audits of the possible five million auditees. No attempt is made to distinguish between misinterpretation and non-compliance, although less than 30% is estimated to be blatant dishonesty. If fraud is not suspected, the auditor does an assessment and imposes a fine.
- If fraud is suspected on the basis of willful concealment of income, the Special Investigation Unit (S.I.U.) carries out a seize and search procedure which may require the presence of the R.C.M.P. with a search warrant. The difference between the two types of audit is one of depth.

The S.I.U. accepts only the cases it can prosecute and win. Some 400 officers investigate approximately 900-1000 cases per year, many of which span up to four years to prosecution. Approximately 2400 auditors carry out 90,000 audits annually.

The department also undertakes special studies such as checking tuition claims and pre- and post-measures of non-compliance among fishermen to identify the ripple effect of selected enforcement.

Focussing on sectors of the economy (e.g., the scrap metal industry, particular professions) produces a much higher return. Compliance research informs the allocation of resources so that there is minimum coverage of the whole economy and concerted efforts in certain areas. Screening techniques have been developed to identify high risk groups, their income range, percentage of non-compliance and estimated recoverable tax gap.

Despite these efforts, the department feels it cannot identify or deal with such activities as organized crime and prostitution. Also, political considerations bear on the staff resources available for investigating.

Nevertheless, the known level of recoverable dollars is growing (see Exhibit IV-2). Whether this is due to more dishonesty, better measurement techniques, inflation or other changes in the economy is unknown.

EXHIBIT IV-2. Recoverable and recovered tax dollars

	Tax Year		
	1976	1977	1978
Gross estimated recoverable tax	$2.1 billion	$2.3 billion	$2.7 billion
Amount collected through enforcement programs	$550 million	$700 million	$800 million

Exhibit B-4 provides S.I.U. operational statistics for the last three years for which they are available. The relative proportion of corporations and individuals investigated is roughly 1:1, although it is often difficult to distinguish since data are recorded by case. All S.I.U. prosecutions result in convictions and involve cases which may have been initiated 2-3 years earlier. These data suggest that the proportion of recoverable dollars dealt with as criminal fraud is small in relation to the total amount of tax gap.

Remedies for tax evasion usually include the tax owing, a penalty and a fine; imprisonment rarely occurs — perhaps 10 cases per year.

Performance indicators are available. Regular audit procedures recover an average of $1,400 per hour and audits of companies with over $200 million in sales produce $6,000 an hour in Calgary, $3,000 an hour in the rest of the country. The department strives to improve these levels. More research to identify key areas of non-compliance could contribute to this goal. But political considerations often favour an increase in the tax rate rather than risk offending taxpayers with increased surveillance.

7. Misleading advertising and deceptive marketing practices

Section 36 of the Combines Investigation Act deals with offences relating to misleading advertising and deceptive marketing practices. The general public often turns to the department for relief against alleged violations of the Act by suppliers or competitors. However, the Act is not intended to provide quick relief in such situations. Rather, it attempts to maintain a competitive environment in the business community over the longer run. The Act prohibits:

- All representations, in any form whatever, that are false or misleading in a material respect.
- Misleading representations as to the price at which the product is ordinarily sold.
- Charging the higher of two prices clearly shown on a product.

- Advertising a product at a bargain price that the advertiser does not have available for sale in a reasonable quantity.
- Running a contest that does not disclose the number and approximate value of prizes.
- Deceptive marketing practices relating to performance claims, warranties, tests and testimonials, and pyramid and referral selling schemes.

During the year ending March 31, 1980, the courts considered 244 misleading advertising and deceptive marketing cases, concluded 134 proceedings and imposed fines totalling $378,380 representing convictions in 100 cases.

The department does not consider the number of prosecutions or convictions to be a valid indicator of performance. Extensive advertising aims at obtaining compliance from Canadian business. Although the number of cases coming before the department has increased, business is considered to be taking a more serious approach to the area.

The largest companies tend to be the most frequent offenders. And the overall number of offences is roughly proportional to the volume of sales. Many of the offences are considered to arise through negligence rather than fraudulent intent. The department can investigate only about 20% of the total load of complaints (see Exhibit B-5). Supermarkets, particularly in Quebec, have been prominent among the prosecutions in recent years.

8. Non-competitive business behaviour

The Combines Investigation Act attempts to prevent business practices in restraint of trade and the adverse effects of concentration. Categories of activity prohibited under criminal sanctions by Part V of the Act include:

- Combinations to lessen competition.
- Being a party to, or assisting in the formation of, an anti-competitive merger or monopoly.
- Being a party to a sale that discriminates against competitors of a purchaser of an article by granting a discount, rebate, allowance, price concession or other advantage to the purchaser that is not also available to competitors.

Within these categories, two specific criminal offences are bid-rigging and predatory pricing. Bid-rigging occurs when one party agrees to refrain from bidding in response to a call for tender or where there is collusion in the submission of bids. The Act prohibits this activity outright. Predatory pricing policy involves the sale of products at lower prices in one area of the country than in the remaining areas, or the sale of goods at unreasonably low prices, where the effect is to lessen competition substantially or even eliminate a competitor.

Exhibit B-6 shows the trend since 1970-71 in the number of complaints received. The number declined during the course of the seventies to a low of 84 complaints in 1974-75, then climbed over the last five years of the decade to a high of 262 cases in 1979-80. The number of formal enquiries in progress at the end of the year has not changed significantly. But the number of prosecutions or other proceedings commenced has generally risen since 1975.

During the fiscal year ending March 31, 1980, the courts dealt with 49 cases under the Act (excluding misleading advertising and deceptive marketing practices cases):

Price maintenance	— 28 cases
Conspiracy	— 15 cases
Predatory pricing	— 4 cases
Bid-rigging	— 1 case
Obstruction	— 1 case

Eighteen proceedings were concluded during the year. In many cases where a not-guilty plea was submitted, the case was dismissed by the courts of first instance or on appeal. During the year, a total of $128,250 in fines was imposed and six Orders of Prohibition were granted.

The Director of Investigation and Research in the Department of Consumer and Corporate Affairs becomes aware of possible offences through complaints (from 1,100 to 1,300 per annum); ministerial orders (rare); or the Director's investigative activity. An average of 15-20 working days is devoted over a three month period to a preliminary enquiry. Then a decision is made to proceed to a more formal stage of investigation. At this point the department may apply to the Crown for compulsory powers of return of documents, etc. Search warrants must state the reasons for the investigation and specify the information sought. Firms may object to the procedure, and a variety of delaying tactics are available.

A noteworthy trend in documentary evidence has emerged. Until the early sixties, considerable documentation (e.g, minutes of meetings) was discovered. Since that time, relatively little documentary evidence has typically been found.

The extent of undetected offences cannot be estimated. Nor can any precise dollar value be assigned to the societal cost of the offences. However, some attempt is made at the time of sentencing to calculate the costs and to estimate the impact on the market.

The Department has been considering amendments to the legislation.

9. Offences against government assistance to business - the Small Business Loans Act

The Department of Industry, Trade and Commerce initiates and refers investigations of borrowers to the R.C.M.P. Most cases are treated as criminal fraud. Statistics on incidence are not kept since known offences are very few in number — only 15-20 investigations and 1-2 prosecutions per year. Present legislation is considered adequate.

10. Offences against the environment

Investigations focus on industry as the offender; the general public and the environment are the victims. No prosecutions under the Environmental Contaminants Act have taken place to date. However, the department does have a record of offences against air and water pollution regulation. The diffuse nature of these offences prevents any reliable estimate of the loss to society.

Compliance divisions within the Department of Environment are responsible for Acts preventing pollution. Offences against these Acts are treated as crimes or regulatory offences, depending on the legislation.

Some feel that the Environmental Contaminants Act could be more specific. But officials generally agree that existing legislation is sufficient with appropriate amendments made as needed. Better enforcement of existing legislation is a concern, particularly with respect to the problem of double jurisdiction between the federal government and the provinces.

11. Tax rebate discounting offences

The Tax Rebate Discounting Act — a relatively new piece of consumer legislation — provides consumer protection to those individuals who sell their tax refunds to companies or individuals willing to pay them a fraction of the expected tax return.

Prior to regulation, the typical problem was that individuals were being offered an unreasonably small percentage of the expected return. Now, discounters must pay the individual 85% of the estimated refund. Moreover, they must notify the individual of the actual return. This provision ensures that the client collects the appropriate share if the rebate is larger than originally claimed.

Opportunities for fraud arise in three instances:

- The registered discounter may deliberately underestimate the expected tax rebate by excluding some deductions and then fail to inform the individual of the correct return (or hope that the individual will not act on the information).

- Individuals may take advantage of the operation of the system to attempt to defraud the discounter (e.g., change addresses and inform the department, but neglect to re-route the rebate to the discounter).

- Individuals may continue to perform discounting services without informing the department.

Tax discounting is a thriving business and anyone who engages in it is required to conform to the terms of the Act. In 1978, 6,700 transactions were recorded; in 1979, this figure rose to 15,600. And the expectation for 1980 tax returns is even greater. If the discounter does not fill in the required forms and the R.C.M.P. or the Department of Consumer and Corporate Affairs does not hear about violations, then the extent of the illegal or fraudulent behaviour goes undetected. In any case, the number of prosecutions under the Act are few: only one occurred in 1979 (the Act's second year), although many more took place in the first year. These violations were of two types: not providing the required 85% of the rebate claim and not sending the excess within 30 days.

Statistics for 1978 show 55 convictions on 139 charges. Fines totalling $12,000 were levied and over $15,000 in restitution was required. Of the eight business discounters who were charged and found guilty in 1978, only two were in business again in 1979. One was charged subsequently and also found guilty.

Clearly, the full extent of the loss to the general public is unknown. The people hurt by the activity of fraudulent discounters are difficult to reach with publicity.

The department is aware of the loopholes in the legislation; it knows where there should be amendments. The Miscellaneous Statute Law Amendment Act (1981) allowed some changes, but the most significant problems with the legislation remain to be dealt with by specific legislation.

12. Unemployment Insurance fraud

The Control Programs Directorate of the Canada Employment and Immigration Commission (C.E.I.C.) develops procedures and supervises investigations of offences against the Unemployment Insurance Act. These fall into several categories:

- Abuse or misuse — cases where claimants fail to fulfill their obligation to search for work.

- Unemployment Insurance (U.I.) fraud — cases where claimants are working, receiving income and not reporting it.

- Employer non-compliance and fraudulent activity — deliberate failure on the part of employers to submit a Record of Employment or falsification of employment data on those submitted.

- Minor criminal activities — including forgery and uttering, theft of U.I. benefits from the mails, illegal use of Social Insurance Number cards, and other crimes against the rights of individuals or property.

- Major criminal activities — including fraudulent schemes and employee misconduct.

Abuse or misuse is a diffuse problem not practically amenable to investigation. U.I. fraud and employer misconduct are investigated under Sections 121-123 and 128 of the U.I. Act for summary conviction or Section 47 for an administrative penalty. Criminal activity is typically dealt with under Section 338 of the Criminal Code (fraud or conspiracy to).

The control function within CEIC seeks to detect, deter and prevent fraud against benefit payment programs. As of October 1980, Investigation and Control staff across the country numbered close to 600, 490 of whom are in the field.

A number of programs detect misconduct. For instance, a Post-Audit Program compares Records of Employment with benefits. In 1979, this program made 489,672 observations which triggered 253,837 investigations. These investigations established 100,778 cases of overpayments worth $19.2 million. The proportion caused by fraud as opposed to error is unknown. The Post-Audit Program refers approximately 25% of the cases investigated by field staff and 50% or more of the prosecutions.

Investigations under the U.I. Act can be directed towards claimants or employers. Exhibit B-7 summarizes operational statistics for the last three years. Charges against employers are generally for non-compliance in issuing Records of Employment. Two points are evident:

- On the basis of Post-Audit results (i.e., overpayments in approximately 20% of the cases observed), it appears that only a small portion of the total pool of overpayments is actually being investigated and recovered. However, the 1978 Report of the Auditor General estimated that only $69 million of a total of $290 million in overpayments was caused by unreported earnings. Record of Employment errors accounted for $120 million.

- Recent years have seen a decline in investigations and overpayments. Officials feel this is possibly due to the time required to implement several new programs.

Investigation and Control Officers refer minor criminal activity to the local police force with jurisdiction for investigation. Major criminal activity discovered by C.E.I.C. staff is referred to the R.C.M.P. Commercial Crime Branch; local police discovering such activity will handle the case if they have the expertise. The R.C.M.P. investigates approximately 50-75 cases annually.

No reliable estimate of the overall level of criminal activity exists. Identified forgeries of U.I. benefit cheques amount to approximately 5,000 cases and $1.5 million per year. U.I. payments make up 18% of all Government of Canada cheques issued and 45% of all forgeries. Criminal fraud cases involving false identification and multiple claims have, on a number of occasions, involved existing or former C.E.I.C. staff. As well, hard-core fraud artists exploit the ease with which false identification can be obtained and the impersonal nature of U.I. benefit delivery to collect from multiple fictitious claims.

Counter-measures to these weaknesses in the system could include:

- The development of a computerized system to detect high risk cases based on a number of key variables such as failure to file an income tax return.
- Mandatory in-person claim initiation and regular reporting.
- A tightening-up of the Social Insurance Number program through such means as pictures on cards and automatic expiry dates.
- More prosecution as a deterrence measure.
- Mandatory minimum fines for overpayments.
- Legislation of the minimum amount of overpayment to be written off — i.e., not identified in audit programs.

A Strategic Policy and Planning study group is currently examining the issue of tightening up legislation. A program has been developed to identify multiple fraudulent claims. But a number of variables constrain more directed enforcement:

- Existing legislation prevents C.E.I.C. from obtaining Revenue Canada data on whether an income tax return has been filed and whether an employer has paid premiums.
- Political pressure not to institute an automated system which scrutinizes all claims. Unemployment Insurance is a tool for income distribution. It appears that the dollar losses as a result of overpayments and fraud do not justify the social and economic costs of screening out many minor and possibly inadvertent offenders.

C. SUMMARY

The potential loss to society as a result of these offences could be considerable. But the dividing line between intentional and unintentional non-compliance is often not apparent nor of interest. Also, the dollar values attributed to offences frequently reflect varying assumptions. Any attempt to aggregate their impact would be unwarranted in the extreme.

Our survey of government departments provided an overview of offences against government by corporations and individuals and against individuals and other corporations by corporations. Some of these offences are treated as crimes; others are not. Certainly many would fall under widely accepted notions of white collar crime.

We were interested in whether these federal departments might have an interest in our definitional and measurement questions. And frequently they do --in an academic or theoretical sense. Or they may welcome what would amount to a subsidy for their own detection efforts. But if interest is defined as needing incidence data to enhance or facilitate their own activities, little application exists.

In most cases, departments recognize that their available resources generate a certain level of effort with outcomes that are predictable. They are generally aware of the behaviour they wish to prevent and direct their efforts — through investigation, prosecution and preparing legislative amendments to increase compliance — towards that end. But the decision to increase or not to increase the effectiveness of the deterrents is a political one.

V

SELECTED PRIVATE SECTOR ORGANIZATIONS: OFFENCES AND CONCERNS

A. INTRODUCTION

To gain a general understanding of the private sector's views on white collar crime, its incidence, costs and the ability of existing internal and legal structures to deal with offenders, we contacted and interviewed individuals in approximately 20 organizations. The firms were chosen from the nine roughly-defined industry sectors listed below.

- Banking.
- Computer services.
- Insurance.
- Manufacturing.
- Recording and motion pictures.
- Retail.
- Securities.
- Telecommunications.
- Transportation (of goods).

The firms or industry organizations selected were generally medium to large in size. Our intention was to direct our resources to corporate entities large enough to have a potentially broad base of experience to discuss.

Our point of contact varied, but was generally at a fairly senior level. Examples of representatives we spoke with include chief executive officers, chief financial officers, vice-presidents, directors of security, directors of computer security, marketing managers and executive directors of industry organizations.

We introduced the interview in general terms (i.e., "As a representative of your industry...") and reassured interviewees that their responses would remain confidential. Most responded in a cooperative and (to all appearances) candid manner. However, we cannot determine how closely the information provided represents a complete picture.

Interviews were semi-structured, generally following the guide shown in Appendix C. The interviewer was free to adapt the instrument to the particular industry and to extend it where necessary.

The following sections present the interview highlights. First, we discuss the reported incidence of various types of offences by sector and the consequences of detection. We then summarize how the private sector perceives the adequacy of the judicial system in dealing with white collar crime.

B RELATIVE INCIDENCE

Exhibit V-1 presents the reported incidence of our 10 pre-selected types of offence. The observation contained in each cell represents an amalgam of individual responses. Offences coded as "H" indicate ongoing or high frequency problems. Those coded "M" or "L" indicate offences detected with medium and low frequency respectively.

We emphasize that these are descriptive indicators only. They reflect estimates made by different respondents based on individual terms of reference: a situation considered serious by one firm or its representative may not be by another.

1. Banking

The banking industry is concerned with almost all of the offence types covered by our protocol. Specific reference was made to the following problems:

- Theft by bank tellers leads to multi-million dollar losses annually.
- International fraud and forgery pose unwieldy problems in detection and evidence gathering.
- Suppliers to the banks regularly provide "kickbacks" to bank employees in the form of merchandise, meals, liquor, etc.
- Bank employees can use their knowledge of corporate acquisitions and mergers financed by the bank to personal advantage in the stock market.
- Fraudulent loans and forgery are also major ongoing problems in the banking industry.
- Organized crime is often involved when managers of banks in areas where organized crime syndicates are active knowingly perform illegal acts. This problem is particularly acute in international operations.

EXHIBIT V-1. Reported incidence

	Sector								
	Banking	Securities	Insurance	Computer Services	Telecom-munic'ns	Mf'g	Retail	Recording & Motion Pictures	Transp'n
1. Commercial bribery and kickbacks	H	M	L	H	L	M	H		L
2. Embezzlement or self-dealing	H	L	L		L	M	H		H
3. Bank violations by bank officers, employees and directors	H								
4. Securities fraud by insiders trading to their advantage by the use of special knowledge; or causing their firms to take positions in the market to benefit themselves	H	H							
5. Employee petty larceny and expense account frauds	H	L	M	H	H	M	M		H
6. Frauds by computer, causing unauthorized payouts		L			M		L		

EXHIBIT V-1. Reported incidence

	Sector								
	Banking	Securities	Insurance	Computer Services	Telecommunic'ns	Mf'g	Retail	Recording & Motion Pictures	Transp'n
7. "Sweetheart contracts" entered into by union officers				L					
8. Commercial espionage				L	H	H	L		
9. Frauds by sales agents writing false orders to obtain advance commissions		L	L	M			M		
10. Pilferage or theft	H		H	H	H	H	H		H
11. Other (see text)					H			H	

When an offender is detected, industry policy generally prescribes firing those directly involved and seeking restitution whenever feasible. Threat of criminal action, however, may be used as a lever to obtain restitution.

2. Computer services

Our respondents in the computer service industry expressed concern in a number of areas, but reported relatively few instances of detected wrongdoing. Specifically:

- Salespeople and systems analysts become intimately familiar with client growth plans for up to five to seven years ahead. This may open the possibility of exploiting that information on the stock market.

- Theft of both company equipment and computer time by staff was noted as an ongoing problem. Cases were noted in which company computer time was used for such purposes as playing games (e.g., chess) and providing computer service to personal clients.

- As well, theft of time in general by employees (arriving late, leaving early) was noted as a concern.

- A case was described in which an individual was receiving four paycheques after termination notices were not entered into the computer. The individual involved then established bank accounts in the names of the terminated employees in various banks and was then able to withdraw the funds from those accounts and in effect increase his salary. The problem was detected when overspent budgets were identified. The variances traced down to the staff account and when that could not be reconciled, fraud was detected.

- Commercial espionage was noted as a grave concern in facilities where product development takes place.

- A major problem with sales agents writing false orders to obtain advance commissions was also described. A particular case in question involved some hundreds of thousands of dollars, and a number of salesmen. The detection of false orders ultimately resulted in the dismissal of a number of the firm's senior executives.

- Another case involved a small computer being demonstration-tested in a potential buyer's office. The small machine was surreptitiously connected to a larger machine in order to enhance its performance (to exceed specifications).

The firms interviewed reported only informal policies established for dealing with those involved in white collar offences. Depending on the severity of the offence, the most frequent response is to fire the individual(s) involved. They reported great reluctance among senior executives to expose their problem to the authorities. This reflects their concern about the adverse publicity associated with attempting to obtain a criminal conviction.

3. Insurance

Our respondents in the insurance industry reported incidences of the following types of offences:

- Buyers of office supplies accepting kickbacks from suppliers for directing business to them.
- Expense account padding.
- Insurance agents claiming false orders in order to achieve sales goals, and become eligible for bonus trips, whereupon they cancel the orders.
- Pilferage and theft of both company and personal property in insurance company offices is a major ongoing problem.

The uniform response to detected offences is to fire those directly involved. Only rarely do firms call in outside authorities and attempt to obtain criminal convictions.

4. Manufacturing

The offences which most concerned our respondents in the manufacturing sector were the following:

- Bribery and kickbacks by buyers of materials and equipment and by contracting officers have been detected with some frequency.
- Commercial espionage was also reported as a concern in high technology industries.
- Finally, a major problem area is pilferage and theft by employees.

Again, most respondents indicated that detected offenders would be fired. They also expressed a willingness to seek criminal convictions when the value of the losses was sufficiently high, hoping that an occasional conviction would have a deterrent effect on other employees.

5. Recording and Motion Pictures

The recording and motion picture industries offer unique opportunities for white collar crime. Such technological advances as home videotape recorders have increased the range of potential misdeeds. The general problem area is unauthorized reproduction of material for resale. These industries seem prepared to concede that reproduction for personal use is likely uncontrollable (certainly unenforceable). However, the potential cost to these industries of unauthorized use of their copyright materials is enormous. Problems of particular concern to these industries are:

- Counterfeiting of records and tapes for sale (estimated to cost the recording industry $50 million per year in Canada).
- Bootlegging - illegal recording of live performances for subsequent copying and sale.
- "Sound-alike" recordings intended to appear to be original artists and packaged like original artists' recordings.
- Unauthorized use of film videotapes in bars and taverns.
- Unauthorized copying of films and videotapes for sale. Access to originals is gained either in collusion with staff or by copying from a broadcast (e.g., Home Box Office or direct from the satellite).

Since these types of activities are typically undertaken by individuals not employed in the "legitimate" recording and motion picture industry, the industry must rely on the government to protect its interests through regulation and/or the formal legal system. At present, this system is not well-equipped to respond to these types of "crimes."

6. Retail

The fact that retailers deal in cash and in merchandise that can be easily converted to cash leaves them vulnerable to white collar crime. Our respondents were particularly concerned about the following types of situations:

- Buyers have been detected accepting kickbacks from suppliers.
- A contracting officer was found to be inviting contractors to submit inflated invoices. He then received cash or "free" work from the contractors.
- Theft of cash and merchandise by staff is a major ongoing problem.

- Retail clerks have been detected abusing the commission process by writing false sales orders and by making unauthorized price reductions to increase sales.

- Computer-generated customer lists have been sold by staff to competitors.

- Abuse of employee discount privileges to buy merchandise for non-employees is an ongoing problem.

- One major retailer reported that hidden microphones were found in its boardroom. Leakage of information on upcoming sales promotions could be particularly damaging.

All of the firms contacted have an established policy of mandatory dismissal. The performance of the offender's supervisor(s) may also fall under scrutiny. Restitution is sought whenever possible, and criminal prosecution will at least be considered if sufficient evidence is available.

7. Securities

Our interviews in the securities industry were unique in that our respondents represented both the regulatory side and the industry side. These two groups held widely differing views on the extent of white collar crime in this industry. Our respondent charged with the responsibility for regulating the securities industry indicated that the following types of activities occur with some frequency:

- Stock exhangers have been bribed with stocks.

- Individuals with vested interests have been appointed directors in an inordinate number of companies. This could lead to a conflict of interest between companies in competition.

- A recurring concern is that staff of brokerage firms will use their insider knowledge to their own advantage.

- Finally, concern was expressed over the appointment to company directorships of individuals who do not have the background to adequately supervise a chief executive or chief financial officer of the firm. This could expose the firm and the shareholders to risk of fraud or embezzlement by the senior officers since the directors are unable to adequately supervise their activities.

Our interviews with representatives of the brokerage industry suggested quite a different picture. In fact, the only problem described in these interviews involved employees in the investment departments of institutions such as banks who make purchases of the same stock as their firm buys. Since the size of institutional purchases may be fairly large, the price of the stock could increase to the benefit of the employee.

Concern with use of insider knowledge was not echoed in our contacts with employees of brokerage firms. Instead, they reported that their main concern was with the physical security of the securities in their possession. They noted that stolen securities could be left as collateral for bank loans and the banks cannot check the serial numbers routinely to determine whether the loan applicant is the registered owner of the securities.

The firms interviewed respond to wrongdoing with a uniform policy of firing those involved. They noted that in a highly regulated industry such as securities, it is extremely important for firms to ensure that their employees are not engaged in activities which will attract the attention of the regulatory agencies. They recognize that repeated violations of industry codes of behaviour could, in the worst cases, result in the firms losing their right to trade on the exchange.

8. Telecommunications

Until recently, the telecommunications industry in Canada was largely operated as a monopoly. However, current attempts to open at least the hardware end of the business to more competition have also generated new opportunities for aspiring white collar criminals. For example:

- Pilferage and theft of company property, frequently for resale, are ongoing problems.
- Ex-employees have formed their own companies and are able to use their insider's knowledge to the advantage of their own firms.

Our respondents also cited the following activities as being of particular concern:

- Toll fraud (theft of long-distance charges).
- Kickbacks to buyers in their purchasing department.
- Ex-employees have formed their own companies and are able to use their insider's knowledge to the advantage of their own firms.
- Abuse of employee expense accounts is a growing problem.
- Employees have been caught using the company's computer system to play computer games, and to serve private (personal) clients.

- On occasion, unauthorized users have breached the security of the data network to which the company is connected.

Company policy for dealing with detected offenders generally involves only reprimands with dismissal in serious cases. Restitution is sought whenever possible.

9. Transportation of goods

Relatively recent technological advances have reduced the potential for white collar crime in this industry. For example, computerized monitoring of the location of rail box cars had made diversion and theft of goods shipped by rail more difficult for both employees and external thieves. However, opportunities for crime still exist, and the following were cited as ongoing problems:

- Shippers may intentionally undercharge a client in return for personal gain.
- Expense account abuse by mid to upper level staff is extensive.
- Company cars are used for personal travel.
- Internal theft by employees is a major problem.

Disciplinary practices followed in this industry include discretionary dismissal of both offenders and their supervisors. Restitution is also sought whenever feasible. In fact, one case was cited in which an employee offered his pension as recompense. The respondent organization rarely resorts to the formal legal system in part because a very large security/internal policing function is maintained.

C. DISCUSSION

Our private sector interviews both raised and clarified a number of issues of importance to this research effort.

1. "New offences"

Our respondents reported several types of activities as white collar crime which we had not included in our protocol taxonomy. Specifically:

- In the recording and motion picture industries, technological changes have provided new opportunities for white collar criminals. Potential offences generally involve the unauthorized reproduction of audio or visual materials for commercial use or resale. While certain of these offences are presently illegal under the Copyright Act, penalties in Canada are so light that enforcement is very unproductive.

- In the telecommunications industry, deregulation has opened the market to suppliers of equipment which can be "interconnected" to existing lines. At present, it is not feasible to monitor lines for the presence of unreported equipment. This results in revenue losses for the utility.

- Several respondents reported the problem of individuals using "lost" or stolen securities as collateral for bank loans. Such securities can be left dormant in banks indefinitely since the banks typically make no effort to determine whether the loan applicant is the registered holder of the securities.

- Theft of computer time by employees was mentioned a number of times. The time stolen can be used for such purposes as doing private consulting work for personal clients or playing computer games.

- The potential for sabotage of computer systems by disgruntled employees (or ex-employees) is a concern in some sectors. The potential dollar losses here are considerable. At the same time, none of our respondents indicated that such sabotage had actually occurred to their knowledge. A related problem is the concern that employees who leave the firm take with them information of potential value to the firm's competitors.

With the exception of the dormant securities problem, the offences listed above are all products of relatively new technology. This may explain both their absence in existing taxonomies, and the fact that they may not be covered by current legislation.

2. Lack of reliance on the formal legal system

Our respondents overwhelmingly prefer to deal with detected offenders internally rather than through the formal legal system. The most frequently-cited reasons for this preference were:

- The police don't know the business (of the victimized firm) well enough to gather sufficient evidence to make the court case successful.

- The court process itself is slow, cumbersome and demands too much staff time.

- The penalties imposed by the courts are (in industry's view) insufficient to deter either actual or potential offenders.

- It is easier to obtain restitution by threatening court action than by actually going to court.
- Victimized firms are reluctant to risk public embarrassment and damage to their reputations by reporting their problems to outside authorities.

Consistent with their tendency to handle problems internally, a number of the firms surveyed reported an increased emphasis on preventive measures. Specifically:

- Explicit codes of employee behaviour have recently been issued by several of our respondent firms. These codes clarify company policy on issues such as conflicts of interest, expense accounts, personal use of company property, disclosure of personal investments and penalties for detected misdeeds.
- A number of firms reported recent or pending installation of such computer security measures as access control software, identity verification and physical security enhancement. The purpose of these measures is to prevent rather than detect crimes involving the firm's computers.
- Finally, general security and internal audit functions are receiving greater emphasis and support in several industry sectors. Shearing and Stenning (1979-80) have speculated that at the present time private security personnel may well outnumber the police. In their view, however, the fundamental role of private security is a preventive one based on the relatively greater freedom of private security personnel to conduct surveillance activities. One likely effect of this emphasis on prevention is that the accumulation and reporting of statistics on offence occurences (however defined) would not be a high priority activity.

3. Perceptions of needed legislative changes

Among the firms surveyed, legislative change is perceived to be needed in three general areas. These are:

- **Computers.** There is general agreement that the law regarding computer-related crimes including theft of time and sabotage is either flawed or nonexistent. The police are also generally viewed as being incapable of investigating such crimes due to the technical sophistication of the offences.
- **Recording and Motion Pictures.** Unauthorized reproduction of recordings and films is a major problem for the recording and motion picture industries. At present, penalties are regarded as

totally inadequate e.g., an offence punishable in the U.S. by a $50,000 fine is punishable by only a $200 fine in Canada. Many of this industry's concerns should be alleviated by the proclamation of the new Copyright Act. In the meantime, statistics on incidence and costs of these offences are lacking, and enforcement of existing laws is minimal.

- **Dormant securities.** The extent to which lost or stolen securities are currently being used as collateral for bank loans is unknown. A change in banking regulations requiring banks to verify the ownership of securities used for this purpose would help to reduce the liquidity of such stocks.

VI

RELATED INDUSTRY PERSPECTIVES

A. INTRODUCTION

The previous two chapters discussed the concerns of public and private sector organizations about specific types of offences. In most instances, our respondents had, at one time or another, been the victims of these offences.

We also approached similar types of issues from the perspective of certain occupations and businesses concerned with the prevention and identification of white collar crime, as well as with mitigating its effects when it does occur. In other words, they occupy a third party position with respect to the offender and the victim.

Specifically, we contacted selected representatives from the following areas:

- Accounting.
- Computer security.
- Industrial security.
- Insurance.
- Legal issues.
- Related organizations.

B. ACCOUNTING

1. The role of chartered accountants

Crocker and Kukiel (1981) point out that the accounting profession is in an excellent position to detect and deter criminals. Auditors enjoy public trust in their mandate to report irregularities in financial statements. Indeed, Romney et al (1980) have produced checklists to help auditors identify fraudulent activity and fraudulent individuals. In a recent study, Crocker and Kukiel addressed the question of whether societal trust in accountants is warranted — i.e., do they take action when they observe fraud?

A random sample of 75 auditors responded to a questionnaire that presented 15 different scenarios. Based on the accountants' code of ethics, five sets of circumstances that are illegal or unethical — each generating three particular situations — were used to gauge the subjects' response to fraudulent activity. The authors found that in general, when auditors observe fraudulent or unethical activity, they ignore it or talk to the person involved. Legal authorities or the person's superior are seldom informed.

Our interview with a national firm of chartered accountants confirmed these findings. They emphasize that their role is to see if financial statements are fair. If they do detect fraud, they have probably stumbled across it. In such cases, the severity of the offence governs the response. Auditors will report what appears to be a serious case to the audit committee or owners, asking them to refer the incident to the company's lawyers. The ultimate outcome generally involves firing the offender and notifying the insurance company. Bonding claims now require only proof that money has disappeared, not who was responsible. If an individual has been identified, the insurance company decides whether to prosecute.

Police investigators of fraud have suggested to auditors that they have a responsibility to report crime. But those interviewed do not agree: they feel their primary responsibility is to their client. Most white collar crime is not reported due to the personalities involved, insufficient evidence, cost and disenchantment with the system. Indeed, they share a lack of confidence in police ability to identify what is a criminal fraud. Also, the question of the employer being at fault for giving too much responsibility to an employee often arises.

Vulnerability in the purchasing function is a universal area of risk. But it is an area where outside auditors feel virtually powerless. Their key concern is with misrepresentation in a financial statement (i.e., overstating assets) in order to maintain market value. And they are continually trying to improve its detection.

The Adams Report — The Report of the Special Committee to Examine the Role of the Auditor — concluded that with respect to illegal or questionable acts:

- There is no Canadian definition of the responsibility of auditors.
- It would be "inappropriate to have auditors apply their personal moral standards to their client's activities."
- "All enterprises with public accountability should be legally required to establish, in their by-laws, a shareholder-approved code of corporate conduct."
- "Codes of corporate conduct should provide a procedure whereby the enterprise's lawyers advise the audit committee of any breaches in the law or the enterprise's code of conduct that have come to their attention; the audit committee should then inform the auditors."

- "The C.I.C.A. (Canadian Institute of Chartered Accountants) Handbook should be amended to set out auditors' responsibilities concerning illegal and questionable acts by clients."

- "An audit cannot be expected to provide assurance that illegal acts will be detected. Generally, the further removed an act is from the transactions reflected in financial statements, the less likely it is to come to the auditors' attention or that auditors will recognize its possible illegality."

On the detection of fraud, the Adams Report commented that:

- Auditors cannot guarantee through an audit of the financial statements that an enterprise is free of fraud.

- To be cost-effective, "audits generally involve testing samples rather than checking every item, examining evidence that is seldom conclusive, and relying on internal controls that may be circumvented by fraud or collusion, often cleverly concealed."

- The profession should "inform the business community of the nature of responsibility that auditors can and do take for the detection of errors and fraud."

- "The profession should organize a method of publicizing to all its members new types of fraud and new ways of preventing or detecting it."[21]

2. Fraudulent activity in the expenditure of government funds: the role of the Auditor General of Canada

Auditing standards of the Auditor General of Canada will soon include general guidelines on recognizing and handling suspected fraud. Althoug audit staff do not carry out fraud investigations, a background bulletin has recently been released to enhance awareness and describe office procedures.

Preparation of this document involved a literature search which revealed very few known cases in Canada. Staff orientation will be followed by efforts to develop tools to assist in vulnerability assessment.

No specific activity has prompted this interest other than a general concern within the auditing community. The practice developed is for audit staff to refer cases to the R.C.M.P., but this has not happened to date. Specific audit data on suspected cases are reported to Parliament.

3. The role of the forensic auditor

In contrast to the traditional audit function is the more focussed practice called investigative or forensic accounting. "Investigative accounting" refers to the assessment of accounting evidence as well as the gathering of such evidence. "Forensic accounting" refers to documentation and presentation of the evidence for trial.

We interviewed a partner in a firm which has specialized in this area. Since 1975, the firm has participated in over 400 cases, both criminal and civil, working for the Crown, police, defendant or plaintiff.

Twice a year, the firm offers a 40-hour course designed for Crown prosecutors and police. The course explains the role of accounting in the prosecution of white collar crime and presents 50 case studies, all of which is supported by 900 pages of prepared text.

In describing the special thrust of his work, the partner interviewed suggested that the traditional audit approach — to assess the quality of internal controls and adjust their degree of scrutiny accordingly — is unlikely to uncover much fraud because:

- It tends to underestimate the potential for evading the internal controls.
- Even auditing checks can be readily thwarted in many instances.

These observations were confirmed by the auditors interviewed; audits rarely produce evidence to show that a crime has been committed. For example, an audit of a retail business might reveal stock shrinkage, but will not generally proceed to uncover the cause.

Offences such as fraud are probably more prevalent in small firms since they tend to have the most primitive internal controls.

C. COMPUTER SECURITY

1. A computer security consulting firm

Our respondents in this area are the founding partners of "the only Canadian company exclusively dedicated to computer security consulting." They claimed that reticence is the greatest barrier to improved understanding of the computer security problem. In their experience, the best route to follow is not through data processing personnel, but through the users and controllers of the data processing function — management. Data processing staff tend to regard security consultants as a nuisance at best.

Obtaining information also presents a problem because businesses often cannot provide a history of their computer security problems since very few bother to track them. Computer audits are of little value since they are only likely to be effective when the type of abuse being investigated is known. Other factors also limit research in this area:

- There is no way to safely generalize from the instances uncovered to arrive at a measure of computer crime.
- A historical focus is constrained by the quickly changing nature of the field. For example, the use of software access control packages introduced only a few years ago to enhance security is increasing so quickly that the potential for certain abuses will soon be negligible in many installations.

Research should be proactive, as well as reactive. As computer applications extend beyond accounting functions, different kinds of abuse or crime may surface. For example, more companies are storing product and market-related information in computer systems, providing opportunities for industrial espionage. Indeed, they expect that abuse centering on industrial espionage and theft of proprietary software will increase significantly.

2. The Ontario Provincial Police (OPP) Antirackets Branch

The OPP recently completed a survey of 648 Ontario corporations and institutions which addressed issues of computer crime and security. The response rate — better than 50% -- was high for such a survey. The results indicated that:

- A large majority of respondents consider the possibility of computer abuse to be important and have designated a person to be responsible for computer security.
- In most cases, computer security was a responsibility added to other, usually unrelated, functions.
- A significant number of companies have had multiple examinations done by consultants, internal auditors and/or external auditors. And a majority had undertaken some modification of their system as a result.
- Very few respondents described their computer security systems as "optimum."
- Only 13 companies reported experiencing a loss through computer abuse. The remaining 96% of responding companies checked a "don't know" response. Theft of computer processing time and malicious damage formed two-thirds of the reported abuses.
- Only five of the 13 incidents were reported to the police.

In response to the survey results, the O.P.P. organized a conference on computer crime and security. The conference attracted attendees at the senior management level and was supported and paid for by the Ontario government. A wide range of computer security issues was covered, including computer crime techniques, computer abuse prevention and methods for protecting computer equipment and data. Attendees received a checklist covering questions of protection, detection, recovery and enforcement procedures. The program was well-received and future sessions are planned.

The O.P.P. holds the view that prevention is really the only viable approach to computer crime, largely because detection is so difficult.

3. The R.C.M.P. Security Systems Branch

The Security Systems Branch deals with computer security issues through its Security Evaluation Inspection Teams (S.E.I.Ts). Essentially audit groups, these teams are responsible for the security of all computer systems within government, as well as private industry systems under contract to the government, dealing with national security and sensitive government information.

Each S.E.I.T. audit results in recommendations on departmental deficiencies. A consolidated report covering all areas of security indicates those areas where the department is not adhering to standards. The team then maintains contact with the department while recommendations are implemented.

The S.E.I.T. group reports to Treasury Board annually on all departments inspected and their progress in implementing recommendations. An attempt is made to review each department or agency every five years.

The Officer-in-Charge of the Security Systems Branch is also the chairperson of the Interdepartmental Computer Security Panel, a sub-committee of the Security Advisory Committee. Most federal departments with major computer installations or contracted services are represented. The Panel's main priority is to tighten the system so that it protects sensitive information. Confidentiality, availability of back-up systems and integrity of data are key elements. The Panel develops EDP standards and practices to guide all government facilities. These guidelines become the S.E.I.T.'s working document — team members look for compliance in the departments being examined.

The standards developed are sufficiently general to apply to all departments and are approved through the government standards group of Treasury Board. They deal with all major areas of EDP operation including software security (e.g., how to prevent unauthorized access), hardware security (e.g., how to isolate systems dealing with sensitive information), operations security (e.g., systems for handling classified documents), etc.

Some standards are written as directives, others are discretionary. But Treasury Board can apply pressure if departments don't comply.

The Security Systems Branch provides security assistance to agencies and departments as an offshoot of their major activity — training programs in computer, environmental and physical security. The EDP security systems staff also trains commercial crime officers in methods of investigating fraud involving computers. They even become involved in the building security program since many building control systems involve microcomputers.

The EDP group is also developing a course to increase the awareness of threats to computer systems among government security officers. For example, people often don't realize the exposure of classified information involved in the use of word processors.

Investigative staff call on the EDP security systems group for special help and court purposes as required. However, the demand on their time to date has not been great since relatively few investigations have taken place.

Statistics on violations of computer security are either not available or are differentiated from general R.C.M.P. crime statistics. Efforts to establish such a data set through the force's operational reporting system have been unsuccessful to date.

At present, the computer security systems group feels constrained most by the absence of a legal avenue to attack computer crime. No precedent has been established on the value of information. For example, how does one determine the value of the federal budget, for instance, to a broker or the oil industry? Similarly, if an individual looks at or changes computerized information but doesn't "take" it, there is no legal recourse. If an employee gains physical access to a computer facility, break and enter charges do not apply. For these reasons, the focus is on protection and prevention.

D. INDUSTRIAL SECURITY

Corporate security managers study the range of risks or threats and the vulnerability of the company and its employers, then attempt to develop workable, preventative measures (Robinson, 1981). Growing concern with security measures stems in large part from computer fraud incidents. But the security function concerns itself as well with such offences as theft of proprietary information or corporate espionage, theft of service from utilities, along with physical security issues, etc.

We interviewed the manager of corporate security for a major utility, who is also the President of the Canadian Society for Industrial Security. Membership in the C.S.I.S. numbers 611 across Canada and 160 in Ontario; 110 new members have joined in the past year. The Society views corporate security as a management function, one that is close to an audit function but with more emphasis on prevention than internal auditors typically provide. Indeed, the C.S.I.S. wants to promote professionalism among its members by becoming a certifying body similar to accounting associations. To do so, the Society expects to develop courses to help members keep up with the state of the art (Sigurdson, 1981).

Security problems tend to be industry-specific. Consequently the C.S.I.S. has several special interest groups organized along industry lines. A great deal of information exchange takes place, much of it quite detailed and confidential in nature.

Approximately 60% of corporate security managers have police backgrounds, Bell Canada is an exception: it draws staff from the operations and financial areas and trains them in security. They are then responsible for tracking down long-distance, third-number and credit card frauds (Robinson, 1981).[22] Despite the otherwise common tendency to select ex-police officers, our respondent draws a sharp distinction between the role of corporate security people and that of the police. Corporate security aims at loss prevention and reduction and so governs its activities on more of a cost-effectiveness basis. Police, by contrast, are more concerned with social impacts and prosecution.

E. INSURANCE

Companies protect themselves against the possibility of employees' dishonest acts by purchasing a fidelity bond, sometimes known as "honesty insurance" (INA Corporation). Two types of fidelity bonds exist:

- One is written for financial institutions exclusively and is generally required by regulatory agencies or other bodies.
- The second type applies to all other organizations and is purchased voluntarily.

In the past, fidelity bonds were written to cover specific employees or positions. Now they cover most employees on a blanket basis, protecting the employer from dishonest or fraudulent acts.

Fidelity bonds provide firms with a continuity of coverage, even if the firm changes bonding companies. This safeguards against white collar crime which goes undetected for years. In the case of financial institutions, any loss discovered during the term of a bond currently in force is covered by that bond, regardless of when the loss occurred. In the case of other businesses, fidelity bonds usually include a one-year discovery period that begins after the bond terminates. Any loss revealed during the discovery period will be paid by the insurer who issued the bond. When the discovery period expires, the new bond will provide coverage according to its specific provisions.

Commercial banks usually determine their required coverage by their deposits, securities brokers by their net capital requirements, and savings and loan associations on their assets. General businesses estimate exposure to employee theft against current assets and sales or income. The result is a "dishonesty exposure factor."

Exhibit VI-1 shows premiums, losses and loss ratios for fidelity bonds in Canada over a five-year period. We discussed loss payouts with two of the largest companies in the field. One respondent reported that such payments do not clearly differentiate the kinds of activity these bonds protect against. The coverage and terms of the bonding arrangement vary. And the payments don't usually correspond to the actual loss incurred. In fact, this relationship may be changing with time. In the past, offenders quite frequently made at least partial restitution (i.e., the insurer's payout was below the actual loss). Restitution occurs less frequently today, so payouts are more likely to be closer to the actual loss.

Both firms reported that fidelity bonding typically accounts for a miniscule proportion of their total business. This observation helps to explain the generally poor data sets available — i.e., the superficiality of insurance industry statistics in the fidelity bond area. For example, the leading fidelity bond writer doesn't track its payouts in a way which distinguishes the kind of institution involved. Also, industry-wide statistics are not sufficiently detailed to reflect year-to-year changes in the number of policies and related coverage aspects.

The categorization of losses presents a problem. The larger of our respondent firms classifies losses at the branch level. Unfortunately, it is sometimes done quite sloppily -- e.g., wrong categories, inconsistent interpretations). The branches are autonomous of most head office functions and are only required to report on losses in excess of $50,000. Consequently, to build a useful data set for research purposes would involve gaining access to loss reports and classifying them appropriately. In such a decentralized company, this could be a very time-consuming process.

This firm also has a head office inspection department which aims at loss prevention through helping clients to improve internal control.

F. LEGAL ISSUES

A review of the criminal code was beyond the scope of this study. Nevertheless, we interviewed a small number of respondents with an interest or mandate to assess the adequacy of existing legislation.

1. The Department of Justice

The Criminal Law Amendments Section reacts to issues introduced by:

EXHIBIT VI-1. Five year premium and loss totals for fidelity bonds in Canada

Year	Net Premiums Earned	Net Losses Incurred	Loss Ratios (%)
1976	$ 16,266,273	$ 8,834,075	54.31
1977	$ 22,324,152	$20,454,033	91.62
1978	$ 20,766,698	$11,198,056	53.90
1979	$ 23,725,306	$ 8,505,790	35.85
1980	$ 25,245,114	$16,908,788	66.90
Total	$108,327,543	$65,900,742	60.80

Source: Canadian Underwriter, May 1981, p.36.

- Complaints to the Minister by a concerned group or agency (e.g., the Canadian Bar Association, provincial departments, special interest groups).

- Positions taken by the Law Reform Commission, a federally-funded body appointed by the Minister of Justice.

Subjects relevant to this study which are or have recently been under consideration include:

a) Theft and fraud

The Law Reform Commission recently made recommended changes (largely simplification) to legislation relating to theft and fraud. The Department of Justice has, in response, initiated a more detailed study as background to the criminal code review. Strengthening of the code might emphasize forfeiture, compensation and restitution as penalties. The review will probably retain the existing structure for dealing with theft and fraud, but weed out some offences and simplify the language.

In general, however, existing legislation is generally perceived by law enforcement officials to be satisfactory. A series of landmark cases have plugged holes, especially for fraud. More specialized fraud prosecution and investigation, even at the municipal level, as well as better staff training in commercial areas, has improved effectiveness. The question is one of resources more than legislation — sifting through documentation to provide evidence can consume considerable staff time.

b) Computer crime

The criminal code currently deals with computer-related crimes under existing provisions such as theft, fraud, break and enter, mischief, etc. No specific offences related to computers exist, leaving serious gaps in the strategies available to prosecutors.

For example, the criterion for theft is that an owner has been deprived of whatever has been stolen, either permanently or temporarily. But the criminal code does not view taking information from a computer as depriving the owner of that information and does not place a value on information stored on tape or on paper.

As well, the recent Supreme Court decision — Regina vs. McLaughlin (1980) — established quite clearly that the code cannot deal adequately with theft of computer time. The closest available charge, and the one ruled inapplicable by the court, was theft of telecommunications services.

Recognizing these problems, a private member's bill (Bill C-628) proposes to expand the definition of property to include computer software, programs and data. Specifically, under proposed amendments:

- Theft of computer software and other data, or unauthorized use of computer time, will become criminal.
- Unauthorized altering of computer data will be treated as a property crime involving destruction or mischief.

Legislation against theft of information remains a problem. Taking information from a display screen is now handled by leakage provisions in the Trade Secrets Act. Setting the scope of the legislation is the thorny issue: should the criteria of fraudulently (dishonestly) and without colour of right (absolutely no right) apply only to computerized information or to any type?

c) Need for coordinated data

No consistent set of statistics exists. Data differ from province to province; charges laid vary, as do rates of prosecution. The newly formed Canadian Centre for Justice Statistics will hopefully alleviate this problem in time.

2. The Law Reform Commission

Under its Criminal Procedures Project, the Law Reform Commission is currently completing two studies on investigating crime which focus to some extent on white collar crime:

- An "Electronic Surveillance" study which touches on the subject of white collar crime in relation to investigating large commercial conspiracy cases.
- A "Search With Warrant" study which deals, in a minor way only, with white collar crime (e.g., tracing funds to a bank account and seizing them to make restitution to the victim).

3. The Canadian Law Information Council

The Council is a federal-provincial think-tank which examines the delivery of legal information, carries out related research and issues publications. Current work of interest is in the area of computer crime.

An analysis of gaps in Canadian legal literature revealed the law of computers as a major area of need. Few precedents exist, largely due to the current weakness of the criminal code. Together with the Canadian Bar Association and the Canadian Information Processing Society, the Council issued a communique to the Attorney General of Canada, the attorney general of each province, and the directors of the territorial departments of justice. It expressed concern about the lack of public protection against computer crime in Canada.

The issue could be viewed as a provincial question in relation to the property aspect of information or as a federal question in relation to theft of computer services. Most responses were oriented more towards the criminal side. The quantum leap to consider information as property has not yet been made.

The Council's Executive Director suggests legislative changes to promote reporting: mandatory reporting for auditors, lawyers and the Securities Exchange Commission are key.

Evidentiary concerns are also problematic. Prosecution becomes complex when the offender can program data to be eliminated. Indeed, the rate of diffusion of technology may limit the possibility of seriously pursuing such offenders.

Nevertheless, the area is perceived to be worth quantifying if only to get a political response. Other areas requiring attention include:

- Promotion of a willingness to discuss cases publicly.
- A national program to develop new techniques of investigation.
- Research into concepts like information and property rights and the interpretation of computerized information.

4. Canadian Association for the Prevention of Crime

The Association is a national citizen's organization with provincial counterparts in all provinces and branches in many communities. Prevention is social, educational and community-based, using such forums as congresses, publications and study committees.

The Association perceives non-violent crime to be more pervasive and threatening to Canadian society than violent offences. But its impersonal nature and diffuse effect make it difficult to arouse public interest. The Association has achieved even less success promoting prevention to business.

Suggested strategies for combatting white collar crime include:

- Educational campaigns directed at the public.
- Increased imprisonment.
- Legislated restitution through assuming the offender's assets.
- Dropping the level of proof required from the criminal to the civil level when a criminal charge is laid against a corporation. This change would remove the crippling effect of establishing

the "directing mind and will" and proof beyond reasonable doubt in offences against combines and anti-pollution legislation.

5. Conclusion

Our discussions suggest some broad trends in the legal context of white collar crime:

- A move towards developing new legislation to deal with new types of illegalities associated with technology. Setting the boundaries of such legislation presents some thorny conceptual problems. However, many of the more serious instances of such crime are dealt with under existing criminal code provisions, perhaps requiring amendments to evidentiary clauses.
- A demand for stronger legislation to deal with corporate criminal behaviour.
- A need to simplify and clarify current legislation in the upcoming criminal code review.

G. OTHER RELATED ORGANIZATIONS

Exhibit VI-2 briefly presents the position of a number of industry and institutional bodies in relation to white collar crime. Most express some interest in the subject in relation to their particular industry or mandate. Few can actually quantify this concern in terms of data or research. Nevertheless, taken together, their interest may suggest possible avenues for future research.

EXHIBIT VI-2. Other related organizations interested in white collar crime

	Association or Institution	Interest in White Collar Crime
1.	Administrative Management Society	The members of this international organization are 12,000 middle to senior-level managers involved in administration. The Toronto Chapter has about 250 members representing 200 companies. The members are generally well-placed to be aware of white collar crime incidents and may be amenable to co-operating in research.
2.	Canadian Association of Chiefs of Police	The Association is not undertaking any research of its own on white collar crime, but does advise other researchers and provides liaison with their member forces. Members would be willing to consider such a role in relation to white collar crime.
3.	Canadian Bankers' Association	The C.B.A. has a Security Committee comprised of representatives from members banks. Most of the research done to date has been done in close contact with the R.C.M.P. and deals mainly with violent crime.
4.	Canadian Bar Association - Ontario	This voluntary organization of practitioners has no data and does not carry out research. Although the group would be willing to consider cooperation, some doubt exists over whether research would be of much interest to members or whether they would have anything to offer.
5.	Canadian Chamber of Commerce	The Chamber represents about 3,500 businesses in Canada, most of which have more than 50 employees. White collar crime is on the list of areas to be examined in the next few years. The Manager of the Publications Department is quite enthusiastic about the subject. He has lobbied for an awareness campaign, but internal politics (i.e., fear that the Chamber would appear to be pointing an accusing finger at its members' employees) scuttled the idea. Nevertheless, he does see scope for cooperation in research, particularly if handled with tact and it is clear to members that the research is on behalf of a government agency.

	Association or Institution	Interest in White Collar Crime
6.	Canadian Information Processing Society - Special Interest Group on Computer Security and Abuse	The C.I.P.S. Special Interest Group is a fairly autonomous collection of computer industry personnel interested in security and abuse issues. The group has roughly 100 members and runs meetings at least once a month on topics of interest such as transborder data flow. C.I.P.S. does not do research, but is willing to consider ways to cooperate (e.g., it might allow a survey of its membership). The "National" group based in Ottawa is not active nationally; most of its members are federal civil servants.
7.	Canadian Institute of Chartered Accountants	The C.I.C.A. does not monitor or act as a clearing house on white collar crime uncovered by auditors. The Director of Auditing Research noted that the focus of the chartered account's audit function is on the forms of management fraud that are likely to materially distort financial statements. The C.I.C.A. is not averse in principle to joint research activity, but questions whether firms are likely to share data.
8.	Canadian Manufacturers' Association	The C.M.A. is not involved in activities or programs related to white collar crime, but is amenable to testing the interest of its membership.
9.	Insurance Bureau of Canada	The Bureau has a Statistical Division, but data are not routinely broken down in a fashion useful for social science research purposes. For example, loss incidence statistics for fraud might be available. If so, we would need to obtain permission from the Board of Directors and then pay the cost of retrieving the data. The Security Division does not deal to a great extent with fidelity bonding. Also,the data reporting plan for fidelity bond writing is non-mandatory. The Bureau is considering making the plan mandatory, but this would take years to implement. Direct contact with fidelity bond firms seems feasible since there are less than 20 operating in Canada. However, their data are classified according to policy type, which might not be meaningful.

	Association or Institution	Interest in White Collar Crime
10.	Insurance Crime Prevention Bureau	The I.C.P.B. is an insurance industry organ which deals with property loss prevention -- overwhelmingly, auto theft and fire-related criminal activity. Lesser matters such as vandalism and fraud only come to its attention as an adjunct to these main areas (e.g. fraudulent insurance claims based on arsonists' activity). The Deputy Manager of the Bureau is head of the Canadian Association of Chiefs of Police's Secretariat for the Prevention of Crime in Industry. In 1972, they conducted an informal survey of 100 businesses. Nothing has been done since. He expressed a willingness to cooperate as head of the secretariat, but did not see any role for the I.C.P.B.
11.	Ontario Ministry of Consumer and Commercial Relations - Business Practices Division	The Division investigates a variety of provincial statutes such as The Business Practices Act and The Consumer Protection Act -- i.e., it deals mainly with offences against people. The data collected are confidential by law. However, the respondent could not indicate whether they spot white collar crime on these investigations (and if so, the procedure to follow in alerting police, etc.).
12.	Ontario Provincial Police Antirackets Branch	The Branch is concerned with white collar crime offences, but the statistics it routinely produces are for broad categories, e.g., "fraud." For detection, they rely on tips and referrals. These sources generate an overabundance of work, so alternative ways to search out white collar crime have not been developed. The Branch maintains close liaison with local forces as well as the R.C.M.P. Where a case involves more than one police jurisdiction in Ontario and is outside the R.C.M.P.'s jurisdiction, it becomes an O.P.P. case. The have in-house expertise in areas such as bank and computer fraud and are willing to share this knowledge.
13.	Society of Management Accountants of Canada	The Society awards the Registered Industrial Accountant designation. It is concerned with the development of controls to prevent fraud, but has no relevant research. However, its library is available and the Society would be amenable to cooperative research on relevant aspect of white collar crime.

VII

OPTIONS FOR FURTHER RESEARCH

A. INTRODUCTION

The choices for further research are almost endless. To avoid floundering, we need to anchor the research to a clear set of policy questions and priorities. This final chapter attempts to do so by:

- Presenting some general policy considerations.
- Reviewing American experience in dealing with white collar crime research.
- Setting out some alternative research strategies.
- Outlining in more detail a recommended strategy in line with current priorities.

B. POLICY CONSIDERATIONS

1. Enforcement capabilities

Grant (1980) points out that since illegal activity will invariably exist to some extent in society, a most important political decision becomes the organization of law enforcement activities. And it is the capability of the enforcement system, not its size, that is key. By capability, Grant means the ability to deal with various types of crime. He suggests that the deployment of resources should reflect the broad spectrum of criminal activity so that one class of offenders is not overlooked at the expense of another.

Also, although the public police play the main enforcement role, several other groups are also involved:

- Provincial securities departments.
- Federal government departments.
- The private security industry.
- The community itself.

In assessing the roles each group should play, a distinction can be drawn between violence to the person and offences against property. The police will likely retain the major responsibility for dealing with personal violence.

Non-violent property offences can, in turn, be broken down into what Grant terms "white-collar crime by persons in position of trust in the victimized enterprise" and individually-directed thefts (e.g., burglary). Although he draws on Sutherland's restrictive definition of white collar crime, Grant points out that both the types of property and persons potentially involved in criminal acts have broadened. He also raises the question of whether law enforcement capability has kept pace with these changes, assuming a proportionate role here in relation to other crimes.

In dealing with these questions, public pressure creates a dilemma for policy-makers. The community could assume more responsibility for minor criminal offences, leaving scarce resources for more sophisticated areas of crime. But members of the public cry loudest about the things that affect them in an obvious and personal way.

> "Both overt predatory crime and clandestine fraud and corruption are criminal activities which exact costs upon the social fabric but only the former provides a parade of individually victimized citizens. The result seems to be that in organizing agency-capability at the political level and in allocating resources within the agencies themselves, a general response is always provided to deal with overt predatory crime against individuals. By comparison, only occasional attention is paid to major fraud and corruption which is treated as an atypical phenomenon, often left to the happenstance of discovery by the media, and not regarded as the task of any official body generally to monitor, prevent and detect." (p.11)

This apparent imbalance suggests the need to evaluate resource allocation carefully to provide appropriate capability in all areas.

Indeed, the United States Department of Justice recently responded to this issue by formulating national priorities for white collar crime law enforcement. White collar crime was divided into seven broad categories based on the different groups of victimized institutions and individuals. After consultation with federal departments and agencies involved in investigation and prosecution, specific criminal offences were designated as priorities under each category. The identification of such priorities was aimed at:

- "Improved coordination and allocation of limited federal investigative and prosecutive resources on both the national and district level.

- Better coordination of federal, state and local law enforcement efforts directed toward white collar crime.

- More comprehensive and timely identification of trends or patterns in white collar crime requiring legislative initiatives or special emphasis in the areas of prevention, detection, investigation or prosecution.

- Expeditious development of new and more effective investigative techniques, prosecution practices, and training programs in white collar crime law enforcement.

- Furtherance of consistency and equal justice in federal law enforcement, in conjunction with prosecutive guidelines for United States Attorneys.

- Improved communication between and among law enforcement officials, Congress, the business community and members of the general public concerning white collar crime problems, their impact on society, and appropriate public and private measures for dealing with them." (U.S. Department of Justice, Report of the Attorney General, 1980, p. i)

These objectives can be reformulated into policy questions, which in turn lead to the task of establishing priorities and a research agenda.

2. From policy questions to research

The number of policy items listed above is considerable: allocation of investigative and prosecutive resources; approaches to prevention, detection, investigation and prosecution techniques and training programs; legislative review; coordination and communication, etc. Establishing priorities among them will reflect a number of interests. For example, the various components of the criminal justice system, business organizations and professionals such as economists and psychologists will each have their own concerns.

To illustrate the types of broad choices to be made, Shapiro (1980) suggests that trade-offs may be necessary between:

- Basic and applied research (i.e., between more academic interests and those of policy-makers).

- Descriptive and explanatory research (i.e., the choice between asking "who and how" or "why").

- The short-term or long-term consequences of research (i.e., implementation of findings from alternative research efforts may have immediate or future impact). Also, the research, as well as its impact, raises questions of timing. Will the immediacy of policy questions and limited resources allow long, complex and expensive research designs?

Finally, the decision-maker must place all of these trade-offs in the context of the available research setting(s) and data. Not an easy task. And the broad trade-offs must ultimately expand into more specific choices. Shapiro provides a "smorgasbord" of research topics related to white collar illegality and its control. She cautions that these are broadly stated and just begin to "scratch the surface" (see Exhibit VII-1). But they reflect the types of research issues which demand attention, depending on the policy questions raised.[23]

C. THE AMERICAN EXPERIENCE

1. Federally-funded research

Federally-supported research on white collar crime in the United States has increased dramatically since the mid-1970s. The greatest concentration of funds has been in the Research Agreements Program administered by the National Institute of Justice (Saxon, 1980).[24] Since 1976, Yale University has received approximately $1.25 million for studies on white collar crime which include the following:

- The economics of corruption.
- Transnational commercial bribery.
- Problems of managerial loyalty and the role of insider misconduct in large corporations.
- An analysis of the enforcement activities and practices of the Securities Exchange Commission.
- A study comparing federal prosecutions of white collar offenders with prosecutions of "blue collar" or "street" offenders.
- An examination of attorneys involved in the defence of corporations and/or corporate executives.
- An extensive sentencing study to determine whether there is a disparity in the sentencing of white collar and blue collar offenders.

Aside from this one research program, federal grants have also funded:

- A study of illegal behaviour by large corporations.
- An analysis of white collar crime data sources.
- A study of the enforcement activities of the Internal Revenue Service.
- Two studies of employee theft.

EXHIBIT VII-1. Shapiro's research agenda on white collar illegality and its control

General Perspective	Components
A. The nature, organization and social location of white collar illegality	1. The form and social organization of white collar illegality. 2. The social location of white collar illegality.
B. The normative dimension of white collar illegality	1. Attitudes and values concerning white collar crime. 2. Legal development. 3. Norms and social policy.
c. The enforcement of norms proscribing white collar illegality	1. The development of enforcement organizations. 2. Enforcement strategy. 3. Enforcement policy. 4. Enforcement impact. 5. The cost of enforcement.
D. The disposition and sanctioning of white collar illegality.	1. The nature of case disposition. 2. Prosecutorial success. 3. The nature of sanctions. 4. Deterrence.

Source: Shapiro (1980), p.. iii.

- A "state-of-the-art" review of enforcement actions to control fraud and abuse in government benefit programs.
- A study of federal antitrust enforcement and offenders.
- A study of the nature, prevalence and impact of computer crime.
- An assessment of computer techniques used for controlling fraud in public assistance programs.
- A study of deterrence of automobile repair fraud in California.
- An examination of the nature, extent and characteristics of consumer fraud and of the laws and regulations to control consumer fraud.

Finally, the National Centre on White Collar Crime established in 1977 at the Battelle Law and Justice Study Centre under the direction of Herbert Edelhertz is supported by federal funds. Among other things, this group has conducted various technical assistance projects for improving white collar crime enforcement.

Despite the length of this list, Saxon notes that many of these studies are preliminary analyses to determine the needs for future action or research.

2. The national study of incidence

In 1980, the United States Department of Justice issued a request for proposal for a "Study of the Impact and Incidence of White Collar Crime in American Society." The objectives of the study were to:

- Provide empirical estimates of incidence and the social, economic and political costs.
- Produce empirical data on the perceptions and awareness of the general public and relevant occupational groups on the seriousness of white collar crime.
- Provide estimates of the effectiveness of alternative enforcement policies in deterring white collar criminality.
- Describe social and organizational sources of white collar crime.

The proposed study evolved from a perceived need for a more comprehensive enforcement strategy. It called for a survey of:

- 1200 representative members of the general public over 18 years of age.
- 600 representative members of various occupational groups (government and business leaders and managers).
- 300 representative members of the legal publics (federal judges and attorneys, private attorneys).
- 300 known federal offenders (representative of all recent known offenders).

The study's methodology suggested that asking respondents to report types of offences in which they had been engaged would produce reliable estimates of incidence. The surveys would also provide data on:

- Awareness of white collar crime.
- Sources and correlates of different types of white collar crime, specifically how current laws and regulations create conditions for it.
- Probable effects of law enforcement policies.

The survey data would then be combined with current research on sentencing practices in federal white collar crime cases. The final outputs would be used to weigh the anticipated benefits of alternative enforcement policies against their implementation costs.

At least two invited bidders — Abt Associates Inc. of Cambridge, Massachusetts and Herbert Edelhertz of the Battelle Law and Justice Study Centre — chose not to respond. The proposed budget was substantial — approximately $700,000. But even that level of resources was judged inadequate to satisfy the study's objectives. Moreover, the question of whether the research methodology justified such a level of funding was raised. Eventually the project was cancelled.

The abortive outcome of the proposed U.S. study underscores two notions which have emerged from our own study of white collar crime:

- A broadly-based measure of incidence should not become the "holy grail" of white collar crime research. It is plagued with methodological difficulties which limit its ultimate use.
- Research should advance in supportable stages geared to clearly specified areas of interest. A design which captures all theoretical white collar crime becomes unwieldy and potentially of little value to many people.

D. POTENTIAL RESEARCH STRATEGIES

1. The federal role

Exhibit VII-2 presents a general overview of white collar crime characteristics and the actors involved in its various manifestations. A quick glance reflects two observations that have surfaced previously in this report:

- The criminal justice system seems to be allocating more resources to areas other than white collar crime.
- Institutions — both public sector and private sector — are assuming the bulk of responsibility in dealing with white collar criminality.

What does this suggest for research? It is doubtful that institutions will forfeit their interests in patrolling and controlling these areas. Nor should they. In most cases, they are best-suited to dealing with these types of offences.

The federal role should be to stimulate research on:

- Increasing our knowledge of general areas of white collar wrongdoing in Canada (i.e., particular offence types which can apply across a range of situations).
- Improving identification and enforcement by whichever group assumes the major responsibility.

2. Optional strategies

One possible initiative we examined was the feasibility of developing an inventory of secondary data sources on white collar crime in Canada.

In a lengthy report submitted to the U.S. National Institute of Justice, Reiss and Biderman (1980) presented the findings of their multi-year study of data sources on white collar law-breaking. This document — based on their examination of administrative records and agency audits of some 30 federal agency offices -- aimed at learning why and how available information on white collar crime was generated. Unfortunately, this study did not identify data sources external to the U.S. federal government. In fact it does not even provide a compendium of the data produced within the agencies examined. Instead, the report discusses, in general terms, the institutional barriers to simple use of existing administrative data in researching white collar crime, and recommends an approach to constructing an optimal statistical reporting system.

With respect to currently available data, Reiss and Biderman (1980) report that:

EXHIBIT VII-2. White collar crime: general characteristics and actors involved

Component of White Collar Crime	Defining Characteristics				Agencies Involved		
	Nature of Offender	Nature of Victim	Mode of Victimization	Losses	Detecting	Prosecuting	Punishing
"Stings and swindles	Noninstitutional position: individuals or "rings"	Individuals and organizations	Deception	Primarily economic	Primarily victims	Primarily CJS	Primarily CJS
"Chiselling"	Individuals with institutional positions	Clients or consumers of institution	Deception	Primarily economic	Institution(?) victims(?)	Primarily institutions	Primarily institutions
"Individual abuses of institutional position"	Individuals with institutional positions	Clients or consumers of institution	Exploitation	Primarily economic but also psychological	Institutions; victims	Primarily institutions	Primarily institutions
Embezzlement and employer fraud	Individuals with institutional positions	Institution itself	Deception	Distributed economic losses	Exclusively institutions	Primarily institutions	Primarily institutions
Client fraud	Clients of financial institutions and government	Institution itself	Deception	Distributed economic losses	Exclusively institutions	Primarily institutions	
Influence peddling/ bribery	Individuals with institutional positions	Institution itself	Collusion between outsiders and insiders	Primarily economic	Victims(?) institutions(?)	Institutions(?) CJS(?)	Institutions(?) CJS(?)
Willful institutional noncompliance	Institutions themselves	Society at large	Exploitation of bargaining position	Economic; physical; psychological	Regulatory agencies	Regulatory agencies	Regulatory agencies

Source: Moore (1980), p. 33.

> "There are many and diverse sources of information on white collar violations of law. The number of relevant, routinely collected data sources is great. Yet when taken individually, each presents problems of adequacy, interpretation and use. When taken collectively, they pose substantial problems of collating (linking) the separate sources of information and fall far short of constituting a comprehensive information system on white collar crime" (p.xxxii).

Our contacts in the public and private sectors confirm these observations. In the absence of a uniform statistical reporting system, the development of such an inventory does not seem feasible. The development of such a reporting system would require:

- "That the statistics encompass administrative, civil and criminal matters."
- That "standard definitions and classification procedures for events regarded as white collar violations" be adopted.
- "That ways be . . . found to estimate or account for multiple counts of the same events."
- That agencies be obliged "to report information about white collar violations in ways that permit its merging from different sources" (Reiss and Biderman, 1980, pp. xxxii-xxxiv).

The level of effort required for such a task, assuming that it could be accomplished at all, would be an unwarranted use of resources when weighed against potential benefits.

Based on our initial findings and review of resarch in other jurisdictions, additional research strategies might include:

a) Development of a cost-benefit framework for investigation

Increasing pressure on resources requires careful selection of cases to be investigated. Future research might attempt to develop a framework for analyzing the relative costs and benefits of proceeding with an investigation. Such a framework would allow for different types of white collar crimes to be classified in terms of potential dollar, human and societal costs, and weighed against the value and probability of completing an investigation.

b) Research on non-reporting of white collar crimes

Our preliminary research shows that there is a strong tendency not to report white collar offences to the police. More detailed analysis of the factors involved in such decisions or policies could indicate where corrective action should be taken (eg., in terms of police image, industry knowledge, skills, communication, etc.).

c) White collar crime and new technology

The introduction and accelerating diffusion of new forms of technology have resulted in a number of offences which represent "gray areas" in terms of legislation, identification, prosecution, etc. A future research study could prepare a taxonomy of these activities (eg., the violation of copyright provisions through the use of videocassette technology), predict possible impact, and discuss legislative and enforcement issues.

d) Cooperative research with corporate groups

Our contacts in the private sector revealed a general spirit of cooperation in research that would benefit member organizations. Access to large target groups through such bodies as the Canadian Chamber of Commerce and the Canadian Manufacturers' Association could be used to explore areas of insider misconduct. Research similar to the work done in conjunction with the American Management Association could generate a body of data on the correlates of offences (e.g., relative level of incidence of particular offences in relation to organizational control variables).

The output might be a set of guidelines to help industry improve its own self-regulation (e.g., codes of corporate conduct, personnel screening, internal controls).

e) Research on internal control mechanisms

A more focused offshoot of the above study would be in-depth analyses of control mechanisms. For instance, a study involving in-depth analyses of previously investigated cases could produce more precise data on the effectiveness and vulnerability of accounting systems. Another application is the area of computer security. A survey of users could focus on computer abuse experiences and actions taken to upgrade security. The results could be used to assess what kinds of abuse are likely as systems evolve, ultimately identifying patterns of vulnerability.

f) Prosecution and sentencing

Disparities in the court processing of "white collar" versus "blue collar" offenders require clarification. Punishment through non-legal means may be more severe than would be exacted through the legal system. Perhaps the attitude of the courts underlies the tendency of firms to offer "quick justice" themselves. Research could attempt to compare severity of offences and disposition of cases dealt with inside and outside the official criminal justice system.

g) Exploring the extent and characteristics of consumer fraud

Moore (1980) observes that the fundamental protection against such offences is self-defence and regulatory efforts.[25] Losses are distributed over a group large enough that often individuals do not have the incentive or resources to complain (if they know they have been victimized). Intimate relationships between the regulating agency and the regulatee, along with the difficulties prosecuting corporate entities, frequently compound the problem.

A possible study in this area could begin by obtaining an approximate measure of incidence through available data sources (e.g., consumer associations, federal and provincial agencies) coupled with a random survey of consumers. Then a pilot project could test the utility of directed consumer awareness campaigns and reporting systems (e.g., for automobile fraud, home insulation fraud, misrepresentation of products such as tapes and cassettes, etc.)

h) A comparative review of enforcement activities in government programs

The federal agencies surveyed generally have allocated their resources to maximize the outputs of their investigation efforts. Different techniques have been used by each to control fraud and abuse in government programs (e.g., computerized regression analysis techniques). A review of the effectiveness of these various strategies in both federal and provincial departments and agencies would provide valuable information to other agencies, police involved in criminal cases and comparable organizations in the private sector.

3. Recommended approach

Each of the options presented above represents a valid research question with respect to white collar crime. The decision of which, if any, to carry out will depend on the resources available and the intended clients(s) for research.

However, given our initial concern with the allocation of limited resources to investigation and enforcement, options (a) and (b) appear to warrant more immediate consideration.

APPENDIX A

LEXICON

APPENDIX A

LEXICON[1]

ABUSE OF TRUST -- the misuse of one's position and/or of priviledged information gained by virtue of that position in order to acquire for oneself (or for another in whom one has an interest) money, property, or some privilege to which one is not entitled.

ADVANCE FEE SCHEMES — schemes in which assurances of some future benefit are made, with full compensation to the promisor/perpetrator to be deferred until final performance — but where the perpetrator has no intention of performing or in obtaining full compensation for performance but rather is interested only in obtaining the partial payment requested as a service fee or an advance good faith deposit (often called a "returnable" deposit).

ANTI-TRUST OFFENCES — combinations in restraint of trade, price fixing or other schemes to unlawfully drive competitors out of business; and/or agreements among competitors to share business according to some agreed formula (such as bid-rigging conspiracies and discriminatory pricing agreements); and/or domination of a business area by one or a few enterprises.

AUTO REPAIR FRAUD — a form of consumer fraud involving maintenance service to automobiles.

BANKING VIOLATIONS — violations by insiders or by customers of banks, savings and loan associations, or credit unions. Insider violations generally involve embezzlements or self-dealing (where insiders lend money to themselves or to businesses in which they have an interest, or take bribes or special favors to make loans or to refrain from collecting loans). Violations by outsiders would include false financial statements to induce a bank to make a loan, the use of fraudulent collateral, check kiting, etc.

BANKRUPTCY FRAUD — frauds involving financial insolvency. There are two major types of bankruptcy fraud:

- the scam or planned bankruptcy, in which the assets, credit and viability of a business are purposely and systematically exploited to obtain cash which is hidden by scam operators.
- fradulent concealments or diversions of assets in anticipation of insolvency so they cannot be sold for the benefit of creditors.

BID RIGGING — see COMPETITIVE PROCUREMENT FRAUD.

---

[1] (Source: H. Edelhertz, et al, The Investigation of White-Collar Crime, U.S. Dept. of Justice, 1977)

BUSINESS OPPORTUNITY SCHEMES — one of the most prevalent and multi-varied forms of fraud in which victims are offered the opportunity to make a living, or to supplement their income by going into business for themselves (full or part-time) by purchasing franchises or equipment to manufacture some item, sell merchandise, or perform some service.

Such schemes range from being total shams to being "opportunities" whose promised returns are highly illusory. The operators of these schemes have essentially one goal, which is to acquire the money of subscriber or investor victims.

CHAIN REFERRAL SCHEMES — any scheme in which the victim is induced to part with money or property on the representation that he will make money through inducing others to buy into the same deal.

One common type of chain-referral scheme is the chain-letter; more sophisticated is the "pyramid scheme," in which (for example) the victim is sold a franchise to sell both merchandise and other franchises, with the promise of profits on merchandise sold and commissions, or "overrides," on merchandise sold by any second- or later-tier victim who buys a franchise from him. The profits appear, therefore, to be in selling franchises rather than in selling merchandise. These schemes ultimately collapse of their own weight.

CHARITY AND RELIGIOUS FRAUDS — frauds arising out of the fund-raising activities of charitable and/or religious groups. Three types of fraud situations are observed in this area:

- the bogus charity or religious group — where money is solicited for a non-existent organization or cause, or for a charitable front created for the sole purpose of soliciting funds which will end up in the collectors' pockets.
- misrepresentation of association with a charity or religious group -- where money is solicited on behalf of a legitimate organization or cause by those with no ties to such organization or cause, and who have no intention of giving money to the group.
- misrepresentation of the benefits or uses of contributions -- situations in which those solicited for donations to a legitimate charity or religious organization are not aware that most of the money collected reverts not to the charitable cause but rather is used to cover the cost of professional fund raisers and/or administrative overhead expenses.

CHEQUE-KITING — any of a variety of frauds against banks which depend for success upon the time it takes to clear cheques.

The most common form of cheque-kiting involves the opening of two or more accounts. Balances are built up in each by deposits from the others. Cheques are circulated between accounts, with no money taken out of any account, until at least one of the banks develops confidence in the depositor. Then the depositor takes money out of the bank, depending on the circulation of cheques between the two or more banks, and the several days it takes to clear cheques (especially between different cities), to prevent detection.

COLLATERAL FRAUDS — frauds involving the holding, taking or offering of collateral pursuant to a financial transaction. In many instances these will be banking transactions. Beyond this, however, such frauds may be encountered in connection with any transaction in which security is provided, such as security for private loans, non-existent accounts receivable sold or pledges to factors, etc. In some cases collateral used as security may not belong to the person offering it.

COMMERCIAL BRIBERY — a form of insider fraud or abuse of trust in which an employee or officer of a private enterprise in some government entity is given a bribe or some other valuable consideration, to induce the employee or official to make a purchase, or grant a contract or some special privilege (such as a zoning variance, license, etc.).

COMPETITIVE PROCUREMENT FRAUD — unlawful manipulation of the public or private contracting process. Three main forms of competitive procurement frauds are:

- bid-rigging — a form of illegal anti-competitive conduct in which bidders in a competitive procurement collusively set their bids so as to deprive the bid solicitor of a competitive process. The effect is an administered bidding process in which the winner and the terms and prices of the goods and services involved in the procurement are set by the conspirators rather than by the "competitive" process. Parties to the conspiracy are thus able to divide among themselves a set of procurement contracts and to fix prices for goods and services at the same time.

- bid-fixing — a form of illegal manipulation of the procurement process whereby one bidding party is provided with inside information (by the bid solicitor or an agent thereof) which enables said bidder to gain an unfair advantage over other bidders.

- bribery/kickbacks — situations in which procurement contracts are let on the basis of the payment of bribes and kickbacks to procurement officials rather than on the basis of competitive procurement guidelines.

COMPUTER FRAUD — frauds arising out of the increasing use of the computer to maintain business and governmental records, such as those relating to inventories, accounts payable and receivable, and customer and payroll records.

CONSUMER FRAUD — frauds of the marketplace involving seller misrepresentations to buyers. Common forms of consumer fraud include:

- selling of useless goods or services, represented as beneficial; e.g., "miracle" face creams.

- misrepresentation of product performance, benefits or safety.

- false and misleading advertising.

- failure to service items after sale, including reneging on warranties.

- repair fraud.

- hidden charges with respect to financing, necessary follow-up services, etc.

- weights and measures violations.

COUPON REDEMPTION FRAUDS — frauds which involve cheating manufacturers or merchandisers who promote sales of their products by offering coupons which return part of the purchase price when the products are purchased. Frauds are committed against the manufacturer by amassing large numbers of coupons and submitting them to manufacturers without any bona fide purchases of the products.

CREDIT CARD FRAUDS — frauds arising out of the application for, extension and use of credit cards. Common credit card abuses include:

- use of stolen credit cards.

- false statements in application for credit cards, including application under a false name.

- buying with no intention to ever pay, by use of a credit card which was originally legitimately obtained.

CREDIT RATING SCHEMES — frauds arising out of the application for, extension and use of credit. Common credit-related schemes include:

- sale of good credit ratings to high risk applicants.

- false statements in application for credit.

- creation of false credit accounts for purposes of theft.

DEBT CONSOLIDATION OR ADJUSTMENT SWINDLES — swindles perpetrated against people who are heavily in debt, and against their creditors, by purporting to provide a service which will systematically organize the marshalling of the debtors assets and income to repay all creditors over a period of time, with creditors refraining from pressing for immediate payment of all sums due.

DIRECTORY ADVERTISING SCHEMES — frauds arising from the selling of printed mass advertising services. These schemes are of two basic kinds: 1) impersonation schemes, in which perpetrators send bills to business enterprises which look like those customarily received; and 2) schemes in which it is promised that advertising will appear in a publication distributed to potential customers but where, in truth and in fact, distribution will be limited to the advertisers themselves, if the directory is printed at all.

EMBEZZLEMENT AND FIDUCIARY FRAUDS — the conversion to one's own use or benefit the money or property of another over which one has custody, to which one is entrusted, or over which one exerts a fiduciary's control

EMPLOYMENT AGENCY FRAUDS — fraudulent solicitations of money or fees in order to find employment for, to guarantee the employment of, or to improve the employability of another.

ENERGY CRISIS FRAUDS — frauds arising out of the sale of goods or services related to energy or fuel use, saving, and production.

FALSE AND MISLEADING ADVERTISING — use of untrue or deceptive promotional techniques resulting in consumer fraud.

The following kinds of practices are prominent among those which fall under the heading of false and misleading adverstising:

- advertising as a "sale" item, an item at the regular or higher price.
- misrepresentation concerning the size, weight, volume or utility of an item.
- falsely claiming an attribute which a good or service does not in fact possess.
- misstatement of the true costs of a good or service through the use of confusing payment provisions or otherwise.

FALSE CLAIMS — fraudulent written claims for payment for goods or services not provided as claimed, to public or private entities.

FALSE STATEMENTS — the concealment or misrepresentation of a fact material to the decision-making process of a government entity, with the result that the government entity accepting the false statement is deprived of the opportunity to decide whether or not to follow up on the situation which a truthful presentation of the situation would have allowed.

FRANCHISING FRAUDS — frauds arising out of business opportunity situations in which individuals invest time, talents and money to obtain a business enterprise, relying on others (i.e., the franchiser) to supply at prearranged rates specified goods and services such as necessary business structures, the goods to be sold or materials with which goods can be made, advertising, and an exclusive territorial market or market area for the franchisee's output.

FRAUDS AGAINST GOVERNMENT BENEFIT PROGRAMS — unlawful application for a receipt of money, property or benefit from public programs designed to confer money, property or benefit under specific guidelines.

FUNERAL FRAUDS — class of guilt inducement frauds relying for success on the emotional stress of victims who have lost, or are about to lose loved ones through death.

GHOST PAYROLLS — forms of false claims in which fictitious employees are added to a payroll and payments to these employees revert to the payroll manipulator(s). Fictitious employees are commonly referred to as "ghosts."

GUILT INDUCEMENT FRAUDS — frauds perpetrated via the tactic of inducing guilt or anxiety in the victim concerning his or her relationship or obligations to another person who is significant to the victim (i.e., a child, parent, spouse).

HEALTH INSURANCE FRAUD — fraudulent practices arising in connection with the receipt or provision of health care services under government financed programs. Such frauds are nearly always perpetrated by health care providers (both professionals and facility operators) against the government(s) financing the programs and/or the intended beneficiaries of such programs.

HOME REPAIR OR IMPROVEMENT FRAUDS — frauds arising out of the provision of goods and services in connection with the repair, maintenance or general improvement of housing units.

INSIDER SELF-DEALING — benefitting oneself or others in whom one has an interest by trading on privileged information or position.

INSURANCE FRAUD — fraud perpetrated by or against insurance companies.

Insurance fraud breaks down into the following categories:

1. Frauds perpetrated by insurers against clients/stockholders, eg., failure to provide coverage promised and paid for when claim is made.

2. Frauds perpetrated by insureds against insurance providers, eg., filing of bogus claims for compensation or reimbursement or multiple claims for same loss from different insurers.

INVESTMENT FRAUD — frauds in which victims, induced by the prospect of capital growth and high rates of return, invest money in imprudent, illusory or totally bogus projects or businesses.

LAND FRAUD — a type of investment fraud which involves the sale of land, based on extensive misrepresentations as to its value, quality, facilities and state of development.

LANDLORD-TENANT FRAUDS — unlawful practices involving the leasing or renting of property.

LOAN OR LENDING FRAUD — unlawful practices arising out of the lending or borrowing of money.

MEDICAL FRAUDS — unlawful activities arising out of the provision and sale of bogus, highly questionable or dangerous medical services, cures or medications.

MERCHANDISING FRAUDS — an umbrella term for a broad variety of consumer frauds involving misrepresentations inducing the victims to purchase merchandise which either is not as represented or which in fact will never be delivered to them.

NURSING HOME ABUSES — a variety of frauds perpetrated by individuals who provide institutional nursing and convalescent care to patients, particularly the aged.

PATENT FRAUD — a form of self-improvement scheme which most closely resembles vanity publishing frauds. In patent frauds, individuals are solicited through newspaper advertisements, etc. to send "patentable" ideas or gadgets to fraud operators for "evaluation by experts." The "evaluation" usually involves a fee, or at least "further processing" of the submission may involve a fee, thus an advance fee situation evolves. The fraud operator generally has neither the intention nor the capacity to develop or process a patentable item.

PENSION FRAUDS AND ABUSES — thefts and fraudulent conversions of pension fund assets either by trustees, employers or employees.

POLLUTION AND ENVIRONMENTAL PROTECTION VIOLATIONS — many abuses in the environmental area involve more than violations of specific environmental/pollution control statutes and orders. White-collar crime abuses in this area consist primarily of the making or submitting of false statements concerning the degree of compliance with statutes and regulations for pollution control and in order to cover up violations or lack of compliance with environmental standards. Falsification of test or sample data designed to measure compliance with standards represents another form of white-collar violation in this area.

PONZI SCHEMES — this is a general class of frauds in which the fraud operator uses money invested by later investor/victims to pay a high rate of return on the investments of earlier victims whose money he has already appropriated instead of making the investments represented to them. Such schemes must inevitably collapse because it is mathematically impossible to continue them indefinitely.

PRICE FIXING — illegal combinations by sellers to administer the price of a good or service depriving customers of a competitive marketplace, restraining competition and maintaining an artificial price structure.

PROCUREMENT AND CONTRACTING ABUSES — see COMPETITIVE PROCURMENT ABUSES.

PUBLIC/OFFICIAL CORRUPTION — white-collar crime which generally falls into the category of abuse of trust-type violations involving commercial bribery, collusion with bid-rigging, avoidance of the competitive process in connection with the purchase of goods and services by governmental entities, self-dealing in connection with governmental purchases or grants of franchise to use public property, real estate variances, etc.

PYRAMID SCHEME — the commercial version of the chain letter scheme, used by fraud operators in the selling of phony distributorships, franchises, and business opportunity plans.

REFERRAL SALES SCHEMES — see CHAIN REFERRAL SCHEMES, MERCHANDISING SCHEMES.

REPAIR FRAUD — a form of consumer fraud involving repairs or maintenance services performed on consumer goods.

RESTRAINT OF TRADE — actions, combinations or schemes which interfere with unfettered marketplace transactions. Examples are: price fixing, bribery and kickbacks, dictation of price structure to customers or dealers, exclusive buying arrangements.

SECURITIES FRAUD — fraudulent activities involving the sale, transfer, or purchase of securities or of money interests in the business activities of others.

SELF-IMPROVEMENT SCHEMES — frauds which appeal to the victims' desires to improve themselves personally or financially, by the acquisition of social or employment skills.

SHORT WEIGHTING OR LOADING — purposeful shorting of the volume or quantity of a cargo, accompanied by a false claim (invoice) demanding payment for the full amount.

TAX AND REVENUE VIOLATIONS — perpetrated with the intent to deprive a taxing authority of revenues to which it is entitled or of information it needs in order to make a judgement regarding revenues to which it is entitled, or to avoid admission of involvement in illicit, though profitable, business activities.

VANITY PUBLISHING SCHEMES — schemes which involve eliciting fees from individuals on the promise of promoting their creative "talents" (real or imaginary), or assisting them in the development of said "talent."

WEIGHTS AND MEASURES VIOLATIONS — abusive practices involving the cheating of customers by failure to deliver prescribed quantities or amounts of desired goods. These violations usually involve false statements or claims in which the victim has relied on seller's representation of the delivered quantity in remitting higher payment.

WELFARE FRAUD — abuses associated with government income and family subsidy programs. Government welfare programs can be exploited by applicants who apply for benefits to which they are not entitled, or continue to claim eligibility when they no longer meet the established criteria for such aid. Receipt of monies from claimants by officials procesing welfare claims represents another dimension of this fraud area.

APPENDIX B

STATISTICAL DATA

EXHIBIT B-1 Summary of prosecutions under consumer protection legislation

	Apr.-Sept. 1973	Apr.-Sept. 1975	Oct. 1977 - Mar. 1978
1. Food and Drugs Act			
Number of charges	31	57	36
Firms or individuals convicted	30	46	25
Total fines	$8,100	$12,000	$8,175
2. Weights and Measures Act			
Number of charges	19	49	91
Firms or individuals convicted	16	20	29
Total fines	$2,455	$7,450	$29,395
3. Packaging and Labelling Act			
Number of charges	-	-	53
Firms or individuals convicted	-	-	18
Total fines	-	-	$9,575
4. Precious Metals Marketing Act			
Number of charges	-	28	7
Firms or individuals convicted	-	3	2
Total fines	-	$2,350	$1,450

Source: Drawn from "Prosecution Reports" provided by the Consumer Products Branch.

EXHIBIT B-2 Operational statistics: Adjudications Directorate

	1979-80	1980-81
Cases Investigated		
R.C.M.P.	3,212	2,356
Excise	105	69
Ports	12,398	12,213
Investigation Service	495	466
Total	16,210	15,104
Cases for Adjudication		
R.C.M.P.	716	549
Excise	105	69
Investigation Service	2,684	2,667
Total	3,771	3,543
Cases Decided		
Customs	4,289	2,943
Excise	96	94
Total	4,385	3,307

EXHIBIT B-3 Revenue related to seizures

	1977-78	1978-79	1979-80
R.C.M.P.	$1,467,980	$1,613,354	$1,618,879
Ports	$3,437,110	$6,358,548	$4,134,717
Investigations	$2,559,052	$2,340,970	$3,783,139
Total	$7,464,142	$10,312,872	$9,536,735

EXHIBIT B-4 Operational statistics for the Special Investigation Unit

	1977-78	1978-79	1979-80
No. of cases investigated	990	949	937
No. of prosecutions	176	180	204
Amount of tax increase (between actual and claimed)	$25.7 million	$26.0 million	$27.9 million
Penalty	$ 4.1 million	$ 3.7 million	$ 4.7 million
Fines	$ 3.3 million	$ 2.5 million	$ 4.3 million
Total value of convictions	$33.1 million	$32.2 million	$36.9 million

EXHIBIT B-5 Operations under misleading advertising and deceptive marketing practices provisions

	1976-77	1977-78	1978-79	1979-80
Number of files opened	7850	8078	8091	9431
Number of complete investigations	1895	2113	2135	2234
Completed case convictions	28	70	109	100

Source: Annual Report, Director of Investigation and Research, Combines Investigation Act, for year ended March 31, 1980, pp.71-72.

EXHIBIT B-6 Operational activities of the Bureau of Competition Policy (excluding misleading advertising and deceptive marketing practices provisions)

	1970-71	1971-72	1972-73	1973-74	1974-75	1975-76	1976-77	1977-78	1978-79	1979-80
Number of files opened on receipt of complaints or inquiries in the nature of complaints	255	271	188	165	84	158	143	173	205	262
Formal inquiries in progress at the end of the year	83	86	76	77	81	71	73	76	73	78
Prosecutions or other proceedings commenced	8	6	14	8	7	12	16	24	11	21

Source: Annual Report, Director of Investigation and Research, for year ended March 31, 1980, p.10.

EXHIBIT B-7 Investigations under the Unemployment Insurance Act

	1978	1979	1980
Claimant Investigations			
Investigations finalized	637,305	675,972	563,235
Disqualification or disentitlement	245,143	248,123	192,104
Overpayments	196,284	172,637	145,959
Amount of overpayments	$36,147,707	$38,831,464	$33,142,353
No. Section 47s	50,888	53,730	46,352
Amount of Section 47s	$ 4,025,544	$ 4,395,163	$3,712,125
Prosecutions commenced by U.I.	6,262	6,128	5,104
No. of fines	5,884	4,904	4,876
Amount of fines	$ 1,717,617	$ 1,520,440	$1,435,125
Employer Investigations			
Investigations finalized	12,585	22,781	40,043
Prosecutions commenced	600	380	205
No. of fines imposed	600	410	228
Amount of fines imposed	$ 56,471	$ 47,130	$ 26,220
TOTAL REVENUE	$41,947,339	$44,794,197	$38,315,823
Benefits paid	$4.5 billion	$4.0 billion	$4.4 billion
Claims received	$2.8 million	$2.6 million	$2.8 million

APPENDIX C

CORPORATE INTERVIEW GUIDE

WHITE COLLAR CRIMES: CORPORATE CONCERNS

RESPONDENT:

TITLE:

ORGANIZATION:

DATE:

A. INTRODUCTION

Before I tell you about our study, I would like to ask you whether you are familiar with the concept of white collar crime?

____ Yes ____ No

(If yes)

What is your understanding of the term?

Our first task in this research was to sift through the many definitions of white collar crime that exist. For our purposes, we have defined it as:

A criminal or quasi-criminal act or omission committed without physical force or its threat that leads to money, property, information, business or personal advantage.

Our project sponsors -- the federal Ministry of the Solicitor General and the R.C.M.P. — feel that more research in this area might be needed so that their enforcement efforts can be better directed.

We have spoken to several people in the public sector about offences by individuals and organizations against government and by organizations against individuals. We are now interested in occupational crime or offences by individuals in the course of their occupations.

Before we begin, I want to assure you that our discussion will be kept strictly confidential and the identity of the firm will remain anonymous.

B. TYPES OF OFFENCES AND INCIDENCE

1. Certain types of offences occur more frequently in particular industries or organizations.

   (Hand respondent list of offences and record answers on interviewer's copy).

   Please go through this list with me and indicate whether any relevant activities have been detected in your firm.

2. Are there any other offences that fit our definition of white collar crime which we have omitted?

(If so, enter into space provided).

3. (If any offences are mentioned, go back to each and ask).

For this offence, can you tell me whether it has been detected:

- on one occasion;
- on a few occasions;
- on an ongoing basis?

4. Can you briefly describe how the offence took place? (Use extra sheet if needed).

5. Can you affix a dollar value to these acts?

C. DETECTION

(These questions should be asked whether or not any offences were reported above. Ask respondent to refer to list, including any offences she/he may have added, and record on interviewer's form).

1. Are systems in place to detect such activity?

____ Yes ____ No

2. (If yes)

Briefly characterize them (i.e., do they involve audits, supervisory monitoring, approvals by more than one person, special follow-up and/or checking procedures, etc?).

3. In general, would you say they are:

____ fully satisfactory;

____ partially satisfactory;

____ not at all satisfactory;

____ under review and/or undergoing modification?

4. How would you rate the likelihood of your organization detecting such activity?

____ very likely;

____ somewhat likely;

____ somewhat unlikely;

____ very unlikely?

D. RESPONSE TO DETECTION

(If such activity is detected).

1. Do you have an established policy for dealing with those involved?

____ Yes ____ No

2. a) Does that policy include:	b) What is the nature of the policy?
____ firing those directly involved	____ mandatory ____ discretionary

Comments? ______________________________

____

- firing those who supervised those directly involved?	____ mandatory ____ discretionary

Comments? ______________________________

____

____ taking action to obtain restitution where appropriate?	____ mandatory ____ discretionary

Comments? ______________________________

____

____ taking action to obtain criminal convictions?	____ mandatory ____ discretionary

Comments? ______________________________

____

____ other (specify)	____ mandatory
______________	____ discretionary
______________	
______________	

3. Do you feel there are offences which are not now illegal but should be so that legal action could be taken?

____ Yes ____ No

(If yes).

Please specify:

____

____

____

____

4. Are there illegal acts which your organization chooses to deal with outside the formal legal system?

____ Yes ____ No

(If yes),

Why?

____

____

____

5. Based on your knowledge of your industry and your organization, do you think there are areas where formal law enforcement agencies could be more effective in stopping white collar crime?

____ Yes ____ No

(If yes),

Please specify:

____

____

____

6. Would your organization be interested in participating in pilot projects which attempted to test better enforcement measures?

____ Yes ____ No

(If no),

Why not?

____

____

____

POSSIBLE OCCUPATIONAL OFFENCES

1. Commercial bribery and kickbacks by and to:
   - buyers
   - insurance adjusters
   - contracting officers
   - quality inspectors
   - government inspectors and auditors
2. Embezzlement or self-dealing:
   - by managers or senior officers
   - by employees:
     - : responsible for incoming funds (e.g., cashiers, mail orders)
     - : responsible for outgoing funds (e.g., purchasing, petty cash, payroll accounts payable)
     - : responsible for inventory
     - : responsible for outside work (e.g., sales, delivery)
   - by attorneys, trustees and fiduciaries
3. Bank violations by bank officers, employees and directors.
4. Securities fraud by insiders trading to their advantage by the use of special knowledge,

   or causing their firms to take positions in the market to benefit themselves.
5. Employee petty larceny and expense account frauds.
6. Frauds by computer, causing unauthorized payouts.
7. "Sweetheart contracts" entered into by union officers.
8. Commercial espionage.
9. Frauds by sales agents writing false orders to obtain advance commissions.
10. Pilferage or theft.

OFFENCES AGAINST RESPONDENT ORGANIZATION

Type of Offence	Frequency			Details and Value
	Once	Few Times	Ongoing	
1. Commercial bribery and kickbacks by and to: - buyers - insurance adjusters - contracting officers - quality inspectors - government inspectors and auditors				
2. Embezzlement or self-dealing: - by managers or senior officers - by employees: : responsible for incoming funds (e.g., cashiers, mail orders) : responsible for outgoing funds (e.g., purchasing, petty cash, payroll, accounts payable) : responsible for inventory (e.g., purchasing, shipping, receiving) : responsible for outside work (e.g., sales, delivery) - by attorneys, trustees and fiduciaries				

Type of Offence	Frequency			Details and Value
	Once	Few Times	Ongoing	
3. Bank violations by bank officers, employees and directors.				
4. Securities fraud by insiders trading to their advantage by the use of special knowledge, or causing their firms to take positions in the market to benefit themselves.				
5. Employee petty larceny and expense account frauds				
6. Frauds by computer, causing unauthorized payouts.				
7. "Sweetheart contracts" entered into by union officers				
8. Commercial espionage.				
9. Frauds by sales agents writing false orders to obtain advance commissions				
10. Pilferage or theft				

Type of Offence	Frequency			Details and Value
	Once	Few Times	Ongoing	
11. Other (specify)				

DETECTION

Type of Offence	Systems		Type	Satisfactory				Likelihood of Detection			
	Y	N		Fully	Partially	Not at all	Under review	Very likely	Somewhat likely	Somewhat unlikely	Very unlikely
1. Commercial bribery and kickbacks											
2. Embezzlement or self-dealing											
3. Bank violations (banks only)											
4. Securities fraud											
5. Employee petty larceny and expense account frauds											
6. Frauds by computer											
7. "Sweetheart contracts"											
8. Commercial espionage											
9. Frauds by sales agents											
10. Pilferage or theft											

APPENDIX D

NOTES

APPENDIX D

NOTES

[1] Herbert Edelhertz, The Nature, Impact and Prosecution of White Collar Crime (Washington, D.C.: U.S. Government Printing Office, 1970), p. 3.

[2] Edwin Sutherland, White Collar Crime (New York: Holt, Rinehart and Winston, 1949).

[3] Miriam S. Saxon, White Collar Crime: The Problem and the Federal Response (Congressional Research Service Report No. 80-84 EPW), p. 7.

[4] Marshall B. Clinard and R. Quinney, Criminal Behaviour Systems: A Typology, (Toronto: Holt, Rinehart & Winstong, Inc., 1973), p. 188.

[5] Edelhertz, Nature, p. 3.

[6] Albert J. Reiss and Albert D. Biderman, Data Sources on White-Collar Law Breaking (Washington, D.C.: U.S. Department of Justice, 1980), p. 4.

[7] R.F. Sparks, "White-Collar Crime: The Problem and the Federal Response," in Hearings Before the Subcommittee on Crime of the Subcommittee of the Judiciary House of Representatives, 95th Congress (Washington, D.C.: U.S. Government Printing Office, 1979), p. 166.

[8] Sutherland, p. 9.

[9] U.S. Department of Justice. Report of the Attorney General, National Priorities for the Investigation and Prosecution of White Collar Crime (Washington, D.C.: U.S. Department of Justice, 1980), p. 5.

[10] August Bequai, White-Collar Crime: A 20th Century Crisis (Toronto: Lexington Books, 1978), p. 2.

[11] Susan Shapiro, Thinking About White Collar Crime: Matters of Conceptualization and Research (New York: New York University, 1980), pp. 2-7, 26-28.

[12] Edelhertz, Nature, pp. 73-75.

[13] U.S. Department of Justice, Report of the Attorney General, National Priorities, p. 6.

[14] Shapiro, pp. 20-23.

[15] Reiss and Biderman, pp. 391-394.

[16] Saxon, pp. 8-11.

[17] Donn B. Parker, Crime by Computer (New York: Charles Scribner's Sons, 1976), p. 30.

[18] Peter Watkins, "Computer Crime: Separating the Myth from Reality," CA magazine, January 1981, pp. 45-46.

[19] John P. Clark and Richard C. Hollinger, Theft by Employees in Work Organizations (Minneapolis: University of Minnesota, 1981), pp. ix-xix.

[20] Laura Schill Schrager and James F. Short Jr., "How Serious a Crime? Perceptions of Organizational and Common Crimes," in White-Collar Crime: Theory and Research, ed. Gilbert Geis and Ezra Stotland (Beverly Hills: Sage Publications, Inc., 1980), p. 29.

[21] CA magazine, April 1978, pp. 44-50.

[22] Allan Robinson, "Prevention is the biggest part of corporate security," Financial Post, 30 May 1981.

[23] Shapiro, pp. 58-59.

[24] Saxon, pp. 89-91.

[25] Mark H. Moore, "Notes Toward a National Strategy to Deal with White-Collar Crime," in A National Strategy for Containing White-Collar Crime, ed. Herbert Edelhertz and Charles Rogovin (Lexington: Lexington Books, 1980), pp. 35, 43.

APPENDIX E

BIBLIOGRAPHY

APPENDIX E

BIBLIOGRAPHY

Allen, Brandt. "Embezzler's Guide to the Computer." **Harvard Business Review**, July -August 1975.

Arbose, Jules R. "White collar crime: a growth industry." **International Management**, November 1980, pp.27-30.

"Attorneys General Respond." Forum/editorial. **CIPS Review**, November - December 1980, pp.2-5.

Avison, N.H. "Crime and the Abuse of Power: Offences and Offenders Beyond the Reach of the Law?" In **Sixth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Briefing Book 1, Discussion Papers**. Prepared for the Canadian Participation in the First Preparatory Meeting, 5-6 March 1980, Ottawa.

Bequai, August. **Computer Crime**. Toronto, Lexington: Lexington Books, 1978.

__________. **White-Collar Crime: A 20th Century Crisis**. Toronto, Lexington Books, 1978.

CA magazine, April, 1978.

Canada. Consumer and Corporate Affairs Canada. **Annual Report, Director of Investigation and Research, Combines Investigation Act**, for the year ending March 31, 1980.

Canada, Statistics Canada. **Perspectives Canada III**. Ottawa: Supply and Services Canada, 1980.

"Canadian Business Reluctant to Report Computer Crimes." **Edpacs**, June 1979.

"Canadian Students Convicted for Computer Time Theft." **Edpacs**, February 1979.

Canadian Underwriter, May 1981, p. 36.

Chamber of Commerce of the United States. **White Collar Crime**. Washington, D.C.: Chamber of Commerce of the United States, 1974.

Clark, John P. and Richard C. Hollinger. **Theft by Employees in Work Organizations**. Minneapolis: University of Minnesota, 1981.

Clarke, P.L. Address before the Manitoba Society of Criminology's "Victims of Crime Seminar." 29 November 1980, Winnipeg.

Clinard, Marshall B., and R. Quinney. **Criminal Behaviour Systems: A Typology.** Toronto: Holt, Rinehart & Winston, Inc., 1973.

Clinard, M., P. Yeager, D. Brisette, and E. Harries. **Illegal Corporate Behaviour.** Washington, D.C.: National Institute of Law Enforcement and Criminal Justice, 1979.

"Computer Crimes Increase." **The Globe and Mail**, 18 August 1981, p.3.

Crocker, Olga L., and Edward Kukiel. "Do Codes of Ethics Prevent White Collar Crime?" Windsor: University of Windsor, Faculty of Business Administration, 1981.

Deighton, Suzan. **The New Criminals: A Bibliography of Computer Related Crime.** London: The Institution of Electrical Engineers, 1978.

Edelhertz, Herbert. **The Nature, Impact and Prosecution of White Collar Crime.** Washington, D.C.: US Government Printing Office, 1970.

____________ et al. **The Investigation of White Collar Crime: A Manual for Law Enforcement Agencies.** Washington, D.C.: U.S. Government Printing Office, 1977.

Geis, Gilbert. "Victimization Patterns in White-collar Crime." In **Victimology: A New Focus.** Ed. Israel Drapkin and Emilio Viano. Lexington: D.C. Heath, 1975.

Geis, Gilbert and Ezra Stotland (eds). **White Collar Crime: Theory and Research.** Beverly Hills: Sage Publications, Inc., 1980.

Grant, Allan. "The Police — A Policy Paper." (A Study Paper prepared for the Law Reform Commission of Canada). Ottawa: Supply and Services Canada, 1980.

Hough, J.M. "Designing Out Crime."

Hubbert, James F. "Computer Personnel Frauds." **Edpacs**, March 1979.

"Insurance Decisions: White Collar Crime." Philadelphia: INA Corporation.

Jensen, Henry. "White Collar Crime, A challenge to the R.C.M.P." **Canadian Chartered Accountant**, December 1973, pp.21-25.

Krauss, L. and A. MacGahan. **Computer Fraud and Countermeasures.** Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1978.

Long, Susan B. "Measuring White Collar Crime: The Use of the 'Random Investigation' Method for Estimating Tax Offences." Paper presented to the 1980 Annual Meeting of the American Society of Criminology. 5-8 November 1980. San Francisco.

May, Edgar. "White Collar Crime: Arrest by Appointment." **Police Magazine**, March 1980, pp.27-35.

Moore, Mark H. "Notes Toward a National Strategy to Deal with White-Collar Crime." In **A National Strategy for Containing White-Collar Crime**. Ed. Herbert Edelhertz and Charles Rogovin. Lexington: Lexington Books, 1980.

National Criminal Justice Reference Service. **White Collar Crime** (annotated bibliography). Washington. 182 cited publications from 1978-1981.

Nycum, S.H. "The Criminal Laws Aspects of Computer Abuse." **Journal of Computers and Law**, 5, pp.271-272.

Orland, L. "Reflections on Corporate Crime: Law in Search of Theory and Scholarship." **American Criminal Law Review**, 17, 501 ff.

Parker, Donn B. "Computer-Related White Collar Crime." In **White-Collar Crime: Theory and Research**. Ed. Gilbert Geis and Ezra Stotland. Beverly Hills: Sage Publications, Inc., 1980, pp.199-220.

Parker, Donn P. **Crime by Computer**. New York: Charles Scribner's Sons, 1976.

Protection Canada. "White Collar Crime Booming, Billions Lost to Business and Industry." November 1980, pp.53-58.

Reiss, Albert J., and Albert D. Biderman. **Data Sources on White-Collar Law Breaking**. Washington, D.C.: U.S. Department of Justice, 1980.

Rhodes, Wayne L. "Computer Crime is No Crime At All." **Infosystems**, August 1979.

Robinson, Allan. "Law outdistanced by technology." **Financial Post**, 30 May 1981.

Robinson, Allan. "Prevention is the biggest part of corporate security." **Financial Post**, 30 May 1981.

Romney, Marshall B. et al. "Auditors and the detection of fraud." **The Journal of Accountancy**, May 1980, 63-69.

Ross, Irwin. "How Lawless Are Big Companies?" **Fortune**, December 1980, pp.57-64.

Saxon, Miriam S. **White Collar Crime: The Problem and the Federal Response**. Congressional Research Service Report No. 80-84 EPW, 1980.

Schrager, Laura Schill, and James F. Short Jr. "How Serious a Crime? Perceptions of Organizational and Common Crimes." In **White-Collar Crime: Theory and Research**. Ed. Gilbert Geis and Ezra Stotland. Beverly Hills: Sage Publications, Inc., 1980, pp.14-31.

Shapiro, Susan P. Thinking About White Collar Crime: Matters of Conceptualization and Research. New York: New York University, 1980.

Shearing, Clifford D. and Philip C. Stenning. "The Quiet Revolution: The Nature, Development and General Legal Implications of Private Security in Canada." Criminal Law Quarterly, 22, 1979-80, pp.220-248.

Sigurdson, Albert. "Group promotes wider awareness of security task." The Globe and Mail, 3 July 1981, p.B2.

Sparks, R.F. "White Collar Crime: The Problem and the Federal Response." In Hearings Before the Subcommittee on Crime of the Committee of the Judiciary House of Representatives, 95th Congress. Washington, D.C.: U.S. Government Printing Office (1979), pp.166-167.

Sutherland, Edwin. White Collar Crime. New York: Holt, Rinehart and Winston, 1949.

Taber, John K. "A Survey of Computer Crime Studies." Computer Law Journal, 11, 1980, pp.275-310.

U.S. Department of Commerce. Crime in Service Industries. Washington, D.C.: U.S. Government Printing Office, 1977.

____________. The Cost of Crimes Against Business. Washington: U.S. Government Printing Office, 1974.

U.S. Department of Justice. Report of the Attorney General. National Priorities for the Investigation and Prosecution of White Collar Crime. Washington, D.C.: U.S. Department of Justice, 1980.

____________. National Institute of Justice. White Collar Crime, A Selected Bibliography (annotated). Washington: 1980.

Wagner, Charles R. The CPA and Computer Fraud. Toronto, Lexington: Lexington Books, 1979.

Watkins, Peter. "Computer Crime: Separating The Myth From Reality." CA magazine, January 1981, pp.44-47.

Winslow, Robert W. Crime In a Free Society. (2nd ed.) Encino, California: Dickenson Publishing Company, Inc., 1968, 1973.